18. Wahlperiode

Deutscher Bundestag
Ausschuss Digitale Agenda

Wortprotokoll
der 53. Sitzung

Ausschuss Digitale Agenda
Berlin, den 16. Dezember 2015, 16:00 Uhr
11011 Berlin, Konrad-Adenauer-Str. 1
Sitzungssaal: PLH E.200

Vorsitz: Jens Koeppen, MdB

Tagesordnung - Öffentliche Anhörung

Tagesordnungspunkt 1 **Seite 08**

Öffentliches Fachgespräch zum Thema:
"Effektivierung der Kontrolle des Exports von Überwachungs- und Spionagesoftware auf deutscher und europäischer Ebene und öffentlicher Auftragsvergabe"

a) **Liste der Sachverständigen**

Ausschussdrucksache 18(24)SB23

b) **Fragenkatalog**

Ausschussdrucksache 18(24)SB24

Mitglieder des Ausschusses

	Ordentliche Mitglieder	Stellvertretende Mitglieder
CDU/CSU	Beermann, Maik Durz, Hansjörg Jarzombek, Thomas Koeppen, Jens Nick, Dr. Andreas Schipanski, Tankred Schwarzer, Christina	Hornhues, Bettina Lange, Ulrich Schön (St. Wendel), Nadine Tauber, Dr. Peter Wanderwitz, Marco Wendt, Marian Whittaker, Kai
SPD	Esken, Saskia Flisek, Christian Kampmann, Christina Klingbeil, Lars Reichenbach, Gerold	Bartol, Sören Dörmann, Martin Stadler, Svenja Träger, Carsten Zimmermann, Dr. Jens
DIE LINKE.	Behrens, Herbert Wawzyniak, Halina	Korte, Jan Pau, Petra
BÜNDNIS 90/DIE GRÜNEN	Janecek, Dieter Notz, Dr. Konstantin von	Beck (Köln), Volker Rößner, Tabea

-3-

Tagungsbüro

Deutscher Bundestag

Sitzung des Ausschusses Digitale Agenda (24. Ausschuss)

Mittwoch, 16. Dezember 2015, 16:00 Uhr

Anwesenheitsliste

gemäß § 14 Abs. 1 des Abgeordnetengesetzes

Ordentliche Mitglieder	Unterschrift	Stellvertretende Mitglieder	Unterschrift
CDU/CSU		**CDU/CSU**	
Beermann, Maik		Hornhues, Bettina	
Durz, Hansjörg		Lange, Ulrich	
Jarzombek, Thomas		Schön (St. Wendel), Nadine	
Koeppen, Jens		Tauber Dr., Peter	
Nick Dr., Andreas		Wanderwitz, Marco	
Schipanski, Tankred		Wendt, Marian	
Schwarzer, Christina		Whittaker, Kai	
SPD		**SPD**	
Esken, Saskia		Bartol, Sören	
Flisek, Christian		Dörmann, Martin	
Klingbeil, Lars		Stadler, Svenja	
Reichenbach, Gerold		Träger, Carsten	
Zimmermann Dr., Jens			
DIE LINKE.		**DIE LINKE.**	
Behrens, Herbert		Korte, Jan	
Wawzyniak, Halina		Pau, Petra	
BÜNDNIS 90/DIE GRÜNEN		**BÜNDNIS 90/DIE GRÜNEN**	
Janecek, Dieter		Beck (Köln), Volker	
Notz Dr., Konstantin von		Rößner, Tabea	

Stand: 9. Dezember 2015
Referat ZT 4-Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

-4-

Tagungsbüro

Sitzung des Ausschusses Digitale Agenda (24. Ausschuss)
Mittwoch, 16. Dezember 2015, 16:00 Uhr

Ministerium bzw. Dienststelle (bitte in Druckschrift)	**Name** (bitte in Druckschrift)	**Unterschrift**	**Amts-bezeichnung**
BMDI			
BMI	Ulrike Bo[illegible]		
AA	Rumpff Johannes		LR
BMWi	Richter Andreas		TRA
AA	ROLZANOVA, THOMAS		VS I

-5-

Bundesrat

Land	Name (bitte in Druckschrift)	Unterschrift	Amts-bezeich-nung
Baden-Württemberg			
Bayern			
Berlin			
Brandenburg			
Bremen			
Hamburg			
Hessen			
Mecklenburg-Vorpommern			
Niedersachsen			
Nordrhein-Westfalen			
Rheinland-Pfalz			
Saarland			
Sachsen	Langer	D. L – ger	Ref.
Sachsen-Anhalt			
Schleswig-Holstein			
Thüringen			

Tagungsbüro

Deutscher Bundestag

Sitzung des Ausschusses Digitale Agenda (24. Ausschuss)
Mittwoch, 16. Dezember 2015, 16:00 Uhr

Öff.

	Fraktionsvorsitz	Vertreter
CDU/CSU		
SPD		
DIE LINKE.		
BÜNDNIS 90/DIE GRÜNEN		

Fraktionsmitarbeiter

Name (Bitte in Druckschrift)	Fraktion	Unterschrift
Piallat	BMG Büro	
Liebing	CDU/CSU	
Scheele	Linke	
Pohl/Jörn	Grüne	

18. Wahlperiode

Deutscher Bundestag
Ausschuss Digitale Agenda

Liste der Sachverständigen
Öffentliche Anhörung
am Mittwoch, 16. Dezember 2015, 16.00 Uhr im Saal E.200 PLH

Zum Thema:
Effektivierung der Kontrolle des Exports von Überwachungs- und Spionagesoftware auf deutscher und europäischer Ebene und öffentliche Auftragsvergabe

Unterschriften:

Herr Prof. Dr. Michael Waidner Fraunhofer-Institut für Sichere Informationstechnologie SIT	
Herr Dr. Sandro Gaycken ESMT European School of Management and Technology	
Herr Prof. Dr. Götz Neuneck Institut für Friedensforschung und Sicherheitspolitik	
Herr Dr. Ben Wagner Centre for Internet & Human Rights European University Viadrina	
Herr Christian Mihr Reporter ohne Grenzen e.V.	

Tagesordnungspunkt 1

Öffentliches Fachgespräch zum Thema: "Effektivierung der Kontrolle des Exports von Überwachungs- und Spionagesoftware auf deutscher und europäischer Ebene und öffentlicher Auftragsvergabe"

Der **Vorsitzende:** Liebe Kolleginnen und Kollegen, ich begrüße Sie ganz herzlich zur 53. Sitzung des Ausschusses Digitale Agenda. Wir haben heute ein öffentliches Fachgespräch mit dem Titel: Effektivierung der Kontrolle des Exports von Überwachungs- und Spionagesoftware auf deutscher und europäischer Ebene und öffentliche Auftragsvergabe. Dazu begrüße ich Sie alle ganz herzlich im Saal, freue mich über das große Interesse und begrüße auch diejenigen, die auf www.bundestag.de den Livestream verfolgen. Ich begrüße ganz herzlich zu dieser Anhörung unsere heutigen Sachverständigen, die wir eingeladen haben. Ich begrüße als erstes Herrn Prof. Dr. Michael Waidner vom Fraunhofer-Institut für sichere Informationstechnologie, herzlich Willkommen. Zum anderen Herrn Dr. Sandro Gaycken vom European School of Management
and Technology, ich begrüße auch Sie, Sie sind ja schon bekannt im Ausschuss hier. Herr Prof. Dr. Götz Neuneck, Institut für Friedensforschung und Sicherheitspolitik, auch Ihnen ein herzliches Willkommen. Herr Dr. Ben Wagner, Center for Internet und Human Rights von der European University Viadrina, herzlich Willkommen, und Herr Christian Mihr, Reporter ohne Grenzen e.V., auch Ihnen ein herzliches Willkommen. Ich freue mich auf eine spannende und interessante Anhörung. Einige Informationen zum Ablauf, wie sich die Fraktionen verständigt haben, erhalten Sie jetzt. Zuerst werden die Sachverständigen ein fünfminütiges Eingangsstatement halten, dazu läuft hier immer die Uhr mit. Anschließend gibt es eine erste Fragerunde nach der Fraktionsstärke. Da haben die Abgeordneten drei Minuten Zeit, ihre beiden Fragen zu stellen, entweder an zwei Sachverständige je eine Frage oder zwei Fragen an einen Sachverständigen. Die Fragen werden gesammelt und dann in der Antwortrunde beantwortet. Dafür haben Sie als Sachverständige auch drei Minuten Zeit, um das ein bisschen dynamisch zu gestalten. In der darauffolgenden offenen Fragerunde wird dann auf die gestellten Fragen gleich geantwortet. Bitte nennen Sie dann auch den Sachverständigen, an den die Frage geht. Auch dazu haben die Abgeordneten und die Sachverständigen jeweils drei Minuten Zeit. Es wird ein Wortprotokoll angefertigt, deswegen nutzen Sie bitte die Mikrofone. Das ist wichtig für die Verständigung, damit man das auch letztendlich im Livestream hört. Danach schließen Sie bitte das Mikrofon wieder, damit es keine Rückkopplung gibt. Das war es zum Ablauf, ich eröffne das Fachgespräch und gebe als erstes das Wort Herrn Prof. Dr. Michael Waidner, bitte schön.

SV **Prof. Dr. Michael Waidner**: Vielen Dank. Sehr geehrter Herr Vorsitzender, meine Damen und Herren Abgeordnete, vielen Dank nochmal für die Einladung zu diesem Fachgespräch, die ich sehr gerne angenommen habe. Im Folgenden möchte ich in Form von sieben Leitgedanken auf die Fragen des Ausschusses eingehen. Hoffentlich in fünf Minuten, es können auch fünfeinhalb sein, muss ich gestehen. Der Leitgedanke eins: Technologie gegen Menschenrechte müssen kontrolliert werden. Überwachungstechnologie kann einerseits der legitimen Strafverfolgung, andererseits aber auch der unrechtmäßigen Verletzung von Persönlichkeits- und Freiheitsrechten dienen. Die Werte des Grundgesetzes müssen auch außerhalb Deutschlands geschützt werden. Der Export von Gütern der Informations- und Kommunikationstechnologie, kurz IKT-Güter, die sich vorrangig gegen Persönlichkeits- und Freiheitsrechte richten, muss deshalb bei begründeten Zweifeln an der Menschenrechtslage im Bestimmungsland stets untersagt werden. Bei der Exportentscheidung zur reinen Überwachungstechnologie muss der Schutz der Menschenrechte immer Vorrang haben. Leitgedanke zwei: Technologien für Menschenrechte müssen exportierbar sein. Viele IKT-Güter unterliegen heute der Exportkontrolle, dienen aber vorrangig nicht der Überwachung, sondern vielmehr dem Schutz vor Überwachung und damit dem Schutz der Menschenrechte. Beispiele hierfür sind Verschlüsselung, Technologien zur Erkennung von Angriffen und auch die automatisierte Erkennung von Softwareschwachstellen. Bei solchen Gütern sollte der Schutzgedanke stets Vorrang haben, d.h., sie sollten frei exportierbar sein. Leitgedanke drei: Schutz braucht Forschung und internationale Kooperation. Technisch betrachtet sind Überwachungsprodukte oft schlicht

Angriffswerkzeuge. Man denke etwa an Spionagetrojaner, die Schwachstellen in der IT ausnutzen, um Daten vom Zielsystem abzugreifen und dann an einen Kontrollserver zu übermitteln. Die Verbesserung der Cybersicherheit ist folglich essenziell für den Schutz vor Überwachung. Je sicherer ein IKT-Produkt ist, desto aufwendiger wird es, in dieses einzudringen und so den Nutzer zu überwachen. Cybersicherheit ist ein Hochtechnologiethema. Systematische und frühzeitige Erkennung von Angriffsmöglichkeiten und die Entwicklung von Sicherheitsmechanismen und Schutzkonzepten braucht Forschung und Entwicklung auf internationalem Niveau. Nur wenn sich die Forschung in Deutschland intensiv mit Angriffs- und Überwachungstechniken auseinandersetzen kann, entwickeln und behalten wir die Fähigkeit entsprechende Schutzmechanismen zu entwickeln. Überwachungstechnologien nutzen sehr oft Schwachstellen in IKT-Produkten. Ein zentrales Ziel der Cybersicherheitsforschung ist es deshalb, solche Schwachstellen, also Fehler, von Anfang an zu vermeiden. Leider gelingt das aber selbst den besten IKT-Herstellern nur sehr unvollständig. Und deshalb ist es wichtig, dass die Forschung Methoden entwickelt, solche Schwachstellen schnell zu finden und diese den Herstellern zu melden. Wenn Sie so wollen, die „Goodguys“ müssen schneller sein als die „Badguys“ auf der anderen Seite. Damit dies in der Praxis gelingt, darf es keine rechtlichen Hemmnisse für die Cybersicherheitsforschung geben, insbesondere nicht für die Erforschung von Schwachstellen in IKT-Produkten. Ebenso wenig darf es rechtliche Hemmnisse für die internationale Zusammenarbeit und den Informationsaustausch zur Cybersicherheit geben. Deutschland nimmt in der Cybersicherheitsforschung einen Spitzenplatz ein. Der größte Teil der Forschung findet aber im Ausland statt. Die internationale Forschungskooperation muss bei der Erstellung von Regeln zur Exportkontrolle angemessene Berücksichtigung finden. Leitgedanke 4: Kontrollkriterien müssen der Technologieentwicklung folgen. Die Digitalisierung ist entscheidend für den Erfolg unserer Gesellschaft und Wirtschaft, vergrößert aber zugleich den Anwendungsbereich von Überwachungstechnologien. Man denke nur an Smartcards oder Smartbuildings mit ihren vielfältigen Möglichkeiten der Überwachung ihrer Nutzer. Die Listen für die Exportkontrolle kritischer Güter müssen deshalb kontinuierlich an die neuen Anwendungsgebiete und damit verbundenen neuen Überwachungstechnologien angepasst werden. Die Geschwindigkeit hierfür muss der der allgemeinen Technologieentwicklung folgen. Leitgedanke 5: Marktgetriebene Entwicklung von Überwachungstechnologien. Überwachungstechnologie wird heute praktisch ausschließlich durch kommerzielle Anbieter entwickelt und vertrieben. Prinzipiell ist es zwar vorstellbar, aber nicht empfehlenswert in Deutschland die Entwicklung von Überwachungstechnologien für die eigenen hoheitlichen Zwecke staatlichen Stellen zu übertragen. In der IKT ist die Konkurrenz am internationalen Markt eine der Haupttreiber für Innovation und Qualität. Damit ist zu erwarten, dass staatliche Überwachungsprodukte der kommerziellen Konkurrenz letztlich immer qualitativ und funktional unterlegen wären. Ein weitergehendes, vollständiges Verbot der Entwicklung von Überwachungstechnologie durch kommerzielle Anbieter wäre schwer vorstellbar. Viele Überwachungstechnologien dienen der Strafverfolgung oder völlig unbedenklichen, zivilen Zwecken, so dass ein allgemeines Verbot nicht zu rechtfertigen wäre. Leitgedanke 6: Abwägung und Abgrenzung bei Dual-Use-Gütern. Die EU-Verordnung 428/2009 bezeichnet als Dual-Use-Güter im Prinzip alle Güter, die sowohl für zivile als auch im Prinzip für nichtzivile Zwecke verwendet werden können. Nach dieser Definition haben sehr viele IKT-Produkte einen doppelten Verwendungszweck. Wie schon erwähnt auch solche, die vorrangig dem Schutz vor Überwachung dienen, beispielsweise Verschlüsselung, und deshalb überhaupt nicht der Exportkontrolle unterliegen sollten. Die Chancen und Risiken von IKT müssen deshalb stets gegeneinander abgewogen werden. Eine zu weit gefasste Definition erfasst viel weniger bedenkliche Güter und behindert damit sinnvolle zivile Anwendungen und verteuert und behindert den Export durch deutsche Unternehmen.

Der **Vorsitzende:** Sie müssen ein bisschen auf die Zeit achten oder das für nachher aufheben.

SV **Prof. Dr. Michael Waidner**: Wenn Sie mir zehn Sekunden geben, dann bin ich fertig. Leitgedanke 7 ist der letzte: Kontrollentscheidungen können durch Technik durchgesetzt werden. IKT-Güter können häufig über das Internet modifiziert

werden. Der häufigste Grund sind Softwareupdates. Dazu kommen ihre Beseitigung oder das Nachrüsten von Funktionen. Sehr häufig kontaktieren IKT-Güter auch den Hersteller über das Internet, um sicher zu stellen, dass das Produkt korrekt lizensiert wurde. Scheitert eine solche Überprüfung, so deaktiviert sich das Produkt oder modifiziert seine Funktionalität. Es wäre deshalb zu untersuchen, wie sich diese Prinzipien der Durchsetzung von Lizenzen, also Digital Rights Management auf Überwachungsprodukte anwenden ließen. Durch eine dynamische Deaktivierung könnte man z.B. zeitlich befristete Ausfuhrgenehmigungen realisieren oder bei Änderung der Rahmenbedingungen im Bestimmungsland früher genehmigte Ausfuhren zurückziehen. Zumindest für manche Arten von Überwachungsprodukten könnte man die Anwendung solcher Methoden zur verbindlichen Vorbedingung für die Exportgenehmigung machen. Keinesfalls natürlich darf die technische Kontrolle die eigentliche Prüfung ersetzen oder absenken, damit herzlichen Dank.

Der **Vorsitzende:** Ja, vielen Dank dafür. Herr Dr. Gaycken, Sie sind als nächster dran, bitte schön.

SV **Dr. Sandro Gaycken**: Vielen Dank für die Einladung. Ich will Ihnen kurz einige meiner Eindrücke wiedergeben. Das Erste ist: Die Bedeutung von Überwachungstechnologie kann gar nicht schwer genug eingeschätzt werden. Wir kennen inzwischen ganz viele Kontexte aus autoritären, totalitären Staaten, wo diese Technologien sehr substantiell genutzt werden, um Oppositionelle und Journalisten zu beobachten, zu identifizieren, dies auch sehr frühzeitig und umfassend, sowie um Schwachstellen herauszufinden oder solche einzubauen. Das sind also Sachen, die sich inzwischen sehr weit etabliert haben. Das fing leider unglücklicherweise mit dem arabischen Frühling an, den ja alle für ein ganz entscheidendes Merkmal der Demokratisierung durch das Internet gehalten haben. Aber das war natürlich auch für die autoritären Staaten ein Warnsignal, was das Internet tun kann. Die erste Reaktion war erstmal, dass man das Internet einschränkte, eingrenzte und abschaltete. Die Reaktion danach war dann allerdings unter der Hilfe verschiedener Forscher und Unternehmen, dass man überlegt, wie man das Internet vielleicht zu Kontrollzwecken einsetzen kann. Das ist etwas, das heute sehr stark implementiert wird. Wir haben also inzwischen eine sehr hohe Datenerfassung, die autoritäre, totalitäre Länder lieben, wenn Sie in der Lage sind diese Beherrschung in das Internet reinzubringen. Wir haben hervorragende Erfassung und Erkennung von Kontexten, von Netzwerken, vor allem sehr gute Datenanalysen über verschiedene Anbieter, verschiedene Forschungsansätze und Paradigmen in der IT. Und wir haben infolgedessen natürlich auch ein wachsendes Verständnis der Anwender, eine Evolution unter den autoritären und totalitären Staaten, wie sie dies nutzen und anwenden können und infolgedessen dann auch wieder einen wachsenden Markt aus Anbietern. Das ist also insgesamt eine sehr unschöne Situation in diesen Ländern, die auch sehr schwierig zu beobachten ist, von denen man immer nur durch einzelne Berichte etwas hört, wie vom Citizen Lab in Toronto. Aber wir müssen ganz klar sagen, dass das Internet kein Werkzeug mehr ist für Demokratisierung, sondern sogar sehr gefährlich für demokratische Prozesse in autoritären Ländern ist. Und meine persönliche Meinung ist, doch ganz stark davon abzuraten, das zu benutzen. Auch Gegenmaßnahmen wie Ende-zu-Ende-Verschlüsselung helfen da nicht viel weiter, weil die für Laien einfach sehr schwierig zu beherrschen sind. Da sind viele verschiedene Hürden dabei, wie man das verstehen muss, dass man es richtig einsetzt, dass man die Kontexte kennt und dass man auch seinen Gegner gut einschätzen kann. Viele der autoritären Regime haben dann doch Alliierte, die sehr gut mit Verschlüsselungsumgehungen umgehen können. Das alles zu beherrschen, ist für Laien oft unmöglich. Von daher ist also eine Effektivierung der Exportkontrollen sehr wichtig. Gerade aus dem Westen sind die Exportkontrollen aufrecht zu erhalten und darauf zu pochen, dass da mehr passiert. Die Formulierungen im Wassenaar-Abkommen sind gut, müssen allerdings um verschiedene Kontexte erweitert werden. Das sind Sachen, die auch schon vielfach angemahnt wurden. Die Schwachstellen müssten theoretisch auch mit hinein, denn natürlich werden auch diese genutzt. Auch die fertigen Exploits, also die fertigen Angriffe, müssen mit hinein in die Formulierung. Ganz wichtig sind auch Dienstleistungen, weil es inzwischen immer mehr Firmen gibt, die gar nicht mehr die Tools, sondern einfach vollständige Dienstleistungen anbieten. Da kann man anrufen und sagen,

man möchte etwas Bestimmtes haben und dann kriegt man das ferngewartet und ist damit unter der Exportkontrolle durchgetunnelt. Wichtig ist auch, dass man Forschung und Entwicklung beobachtet. Wir haben also immer wieder gesehen, dass es Schwachstellen gibt, über die man die offene Forschung überwachen kann. Wenn also eine sehr offene Forschung da ist, dann wird das sehr häufig von diesen autoritären Ländern angenommen. Wir sehen gerade in Asien, dass die Forschung sehr viel aus der westlichen Forschung adaptiert und dann sehr viel in diesen autoritären Regimen in entsprechende Technologien umsetzt. Effektivierung ist allerdings sehr schwierig. Der Kontext ist tatsächlich eher wichtiger als die technische Spezifikation. Die Frage der Einsetzung ist sehr wichtig. Das Ganze erfordert auch eine sehr hohe Kompetenz der Behörden. Man muss sehr viel wissen, sehr viel kennen, auch die verschiedenen autoritären Länder sehr gut kennen, denn die sind natürlich auch gerade dabei ihre eigenen Märkte auszubilden. Sehr viele dieser Technologien kommen gar nicht mehr aus dem Westen, sondern kommen aus den Ländern selber. Da ist es dann natürlich entsprechend schwieriger noch einzusehen, was im Detail passiert. Man braucht auch eine gewisse Kooperation der Firmen. Die Weiterverbreitung ist auch in den einzelnen Fällen nur sehr schwierig zu beobachten. Da könnte man aber darüber nachdenken, ob man eventuell Watermarking-Techniken oder ähnliches einsetzt. Zum Schluss will ich Sie noch darauf hinweisen, dass wir neue Trends auch in diesem Feld haben. Einerseits, dass sich die Datenquellen vervielfältigen. Man will also nicht mehr nur den Officerechner von einem Oppositionellen infiltrieren, sondern alles Mögliche, was ihn digital umgibt infiltrieren, um ihn zu identifizieren. Weiterhin haben wir eine deutlich höhere Bedeutung der Datenanalysetechniken. So etwas wie Big Data-Analysen sind in letzter Zeit das Überwachungswerkzeug schlechthin geworden. Wir sehen in Verbindung damit auch eine ganz starke Verbindung mit regulativen und technischen Ansätzen. Meistens versucht man einfach die Daten von den Telekommunikationsprovidern oder irgendwelchen anderen Providern abzugreifen, jagt sie durch Big Data-Analysen und hat dann vollständige Profile. Das ist natürlich alles was nicht von Exportkontrollen aufgegriffen wird. Damit wäre ich erst einmal am Ende.

Der **Vorsitzende:** Vielen Dank, Herr Dr. Gaycken, und jetzt Herr Prof. Dr. Neuneck, bitte schön.

SV **Prof. Dr. Götz Neuneck**: Zunächst vielen Dank für die Einladung hier vor Ihnen zu sprechen. Ich muss vorausschicken, ich bin Physiker und kein Informatiker und begegne der ganzen Materie mehr aus der Sicht der Rüstungsexportkontrolle. Es gibt ein Spektrum von möglichen Gegenmaßnahmen gegenüber exzessiver Überwachung. Die rechtlichen Komponenten diesbezüglich sind natürlich gerade schon genannt worden. Dazu gehören das Wassenaar-Arrangement und die EU, sowie das Dual-Use-Übereinkommen, in dem Dual-Use-Güter erfasst sind. Dieses geschieht in erster Linie unter dem Aspekt, dass Rüstungsgüter in bestimmte Regionen nicht transferiert werden sollen. Allerdings ist der Begriff ausgeweitet worden. Er umfasst inzwischen auch sogenannte Intangibles, also Dinge, wie Software, Brookering und Faxe. So gesehen hat sich auch international durchgesetzt, dass der Begriff Dual-Use-Gut sehr weit gefasst ist. Es geht darum, dass Überwachungstechnologie schon heute genehmigungspflichtig ist. Die Frage ist, ist die Genehmigungspflichtigkeit effizient? Was sind die Kriterien, die dem zu Grunde liegen? Wo entsteht Missbrauch und wie kann man dem entgegengehen? Wichtig ist die Strafandrohung und ein gewisser Reputationsverlust derjenigen, die dem zuwiderhandeln. Es gibt bis heute kein internationales Regime. Man könnte davon ausgehen, dass es in Zukunft so eine Art Code of Conduct gibt, also Abkommen, die so etwas berücksichtigen können. Der Arms Trade Treaty versucht den Fluss von Rüstungsexportgütern zu erfassen. Dieser bezieht sich aber in erster Linie eben auf klassische Rüstungsexportgüter. Es wäre sicherlich eine Idee, diesen Begriff auch auszuweiten auf Dual-Use-Güter. Die Kriterien, die dem zu Grunde gelegt werden können, sind Völkermord, Angriffskrieg und schwere Menschenrechtsverletzungen. Unter diesen Bedingungen sollten eben solche Exporte nicht vorgenommen werden. Es gibt ein Spektrum von Möglichkeiten, um so etwas einzudämmen, damit Überwachungstechnologien weder für die Kriegsvorbereitung noch für innere Repressalien benutzt werden können. Die rechtlichen Instrumente sind sicherlich erweiterbar. Die Praxis spricht dann aber letztlich die Wahrheit darüber, wie das tatsächlich auch von anderen Staaten gehandhabt wird. Das

Wassenaar-Abkommen hat nur 40 Mitglieder. Die Möglichkeiten der EU sind begrenzt. So gesehen deutet der Hinweis, dass andere Staaten auch liefern könnten und dadurch Druck auf Hersteller, die im eigenen Land tätig sind entsteht und diese sagen könnten, dadurch würden sie die Kontakte verlieren, im Grunde genommen darauf hin, dass man das globale Problem eigentlich nur international lösen kann. Welche Möglichkeiten bestehen? Die erste Möglichkeit ist, die Wahrnehmung der Hersteller zu verbessern. Das kann die Wahrnehmung einerseits der Eigenverantwortung und andererseits der ethischen Gründe in bestimmte Länder nicht zu liefern, sein. Da spielen Länderlisten eine ganz gewaltige Rolle, die natürlich erstellt werden müssen und das allein ist ein schwieriger Prozess. Die zweite Möglichkeit ist, sich die Frage zu stellen, was man bei einem Verstoß tut? Wie wird der Verstoß nachgewiesen? Wie funktioniert die Analyse bezogen auf den Vorfall? Man hat auch manchmal gar nicht die richtigen Informationen. Weitere Möglichkeiten wären, Software zu klassifizieren oder zu zertifizieren, also letztlich zu kennzeichnen oder eine gewisse Form von Meldepflicht generell einzuführen. Man kann natürlich auch technisch an solche Dinge wie Einbau von Lockdateien oder von Telemetriedaten denken, aber das wirft natürlich wieder die problematische Frage auf, ob die Lieferung von Überwachungstechnologien selbst überwacht werden können. Damit hat man wieder einen ganzen Rattenschwanz von Problemen. Aber als Möglichkeit muss man es, meines Erachtens, zumindest nennen. Dann kann man natürlich darüber reden, ob man nicht Firmen zertifizieren könnte, die bestimmte Technologien liefern oder indem man Verantwortliche dieser Firmen nennt, die dafür verantwortlich sind, dass es erstens zu einer Zertifizierung kommt und zweitens, dass es nur zu Lieferungen in Länder kommt, die ein legitimes Interesse haben sowie legal und verantwortungsvoll mit der entsprechenden Software umgehen. Heute gibt es eine Art von Exportprüfung. Ich überspringe das, weil meine Zeit jetzt auch schon wieder abgelaufen ist. Es gibt mehrere andere Möglichkeiten der Kontrolle, zum Beispiel Hermesbürgschaften oder Industrieförderung. In dem Moment, in dem man in Entwicklung und Forschung investiert, muss man sich dann natürlich auch fragen, wo diese Informationen, Software usw. gelangen, also in welche Staaten. Als Letztes wäre der Vorschlag, eine Art von Güter-Empfänger-Matrix zu erarbeiten, in der bestimmte Güter für bestimmte Empfängerländer in Ordnung sind und andere nicht. Darauf kann ich dann eingehen, wenn später Zeit ist.

Der **Vorsitzende:** Vielen Dank, Herr Prof. Dr. Neuneck. Und jetzt hat Herr Dr. Wagner das Wort, bitte schön.

SV **Dr. Ben Wagner**: Vielen Dank für die Einladung und auch, dass Sie sich dieses Themas angenommen haben. Ich weiß, es ist ein sehr technisches Thema und auch durchaus relativ komplex, was die Materie angeht. Deswegen ist es umso wichtiger, dass gerade solche technischen Themen in solchen Runden besprochen werden. Ich würde, wie bereits meine Vorredner, erst mal darauf eingehen, dass man grundsätzlich die zentrale Rolle von Überwachungstechnik bei Menschenrechtsverletzungen anerkennen muss. Und das ist sehr relevant, nicht nur für manche Aktivisten oder für bestimmte Journalisten, sondern für Gesellschaften an sich. Wenn Gesellschaften sich überwacht fühlen, hat das bestimmte Konsequenzen und es wirkt sich natürlich auch auf die Gesellschaft in der Gesamtheit aus. Man muss auch sagen, dass sich die rechtlichen und auch die tatsächlichen Rahmenbedingungen nach dem Snowden- und NSA-Skandal international deutlich verschärft haben. Es ist so, dass wir vielleicht von bestimmten Fortschritten in westlichen Demokratien reden können. Im Einzelfall ist es international eher so, dass man das Anwachsen von Mini-NSAs oder Mini Government Communications Headquarters in aller Welt beobachten kann. Und vor diesem Kontext ist es natürlich besonders wichtig, dass es Rückschritte im Bereich der Menschenrechte gibt. Es ist auch wichtig, wie man damit umgeht, wenn deutsche und europäische Technologie exportiert wird und dazu genutzt wird, dass Menschenrechtsverletzungen in aller Welt begangen werden können. Und da gibt es zwei sehr relevante Beispiele, die sehr gut dokumentiert sind. Erstens in Syrien und zweitens in Libyen, wo während der Auseinandersetzungen europäische Firmen im E-Mail-Kontakt mit entsprechenden Menschen vor Ort, die von der örtlichen Regierung sind und fragen: Ihr habt da ein Problem mit einem Aufstand, was können wir

tun? Das ist jetzt natürlich etwas überspitzt formuliert, aber man kann sich ungefähr vorstellen, dass bei solchen Firmen die Eigenverantwortung etwas komplexer zu gestalten ist und man nicht nur mit freundlichen Corporate Social Responsibility-Richtlinien oder netten, unverbindlichen und letztlich wenig effektiven Corporate Social Responsibility-Maßnahmen kommen kann. Und da ist natürlich die Frage, wie man damit umgeht. Es gibt den Bereich der Exportkontrolle und es hat relativ lange gedauert auf deutscher und europäischer Ebene bis man da entsprechende Lösungen entwickelt hat. Und jetzt haben wir einen ersten Schritt auf internationaler Ebene über das Wassenaar-Arrangement, der es zumindest versucht, das zu erfassen. Das ist ein erster wichtiger Schritt und wie meine Vorredner würde ich auch betonen, dass da Weiterentwicklungen notwendig sind. Es gibt eine Debatte über die Qualität der bestehenden Definition im Bereich von Intrusion Software, die man ernst nehmen muss. Da kann ich zum Beispiel die Arbeiten von Sergey Bratus, aber auch anderen Forschern in dem Bereich empfehlen, die sich mit diesen Themen befasst haben, weil es wichtig ist, dass man sicherstellt, dass auch bei einer neuen Regulierung keine Fehlanreize gesetzt werden, zum Beispiel um Sicherheitsforschung einzudämmen oder einzuschränken. Gleichzeitig ist es aber auch so, wie schon genannt worden, dass die verschiedenen bereits bestehenden Einschränkungen von kryptographischer Technologie in der Form, wie sie jetzt vorhanden sind, aus Menschenrechtsperspektive nicht sinnvoll sind. Es ist sogar so, dass verschiedene Unternehmen, sowohl in Europa als auch in Deutschland, eine stärkere Lockerung von Regulierung in der Exportkontrolle von Kryptographie entweder über General Export Authorisation (GEA) oder über eine komplette Deregulierung über Wassenaar fordern. Es gibt verschiedene Möglichkeiten, wie man das machen könnte. Es sind aber verschiedene Präzisierungen der bereits bestehenden Regulierungen, die durchaus sinnvoll wären. Was schon von Herrn Prof. Dr. Neuneck in Bezug auf das Arms Trade Treaty und was noch kommt genannt worden ist, ist auch ein bisschen nach vorne schauend. Wir haben einen Bereich, der sehr stark und sehr lange diese Frage von zivil oder militärisch diskutiert hat. Es ist wichtig, jetzt auch in den neuen Verträgen, die jetzt kommen werden, insbesondere im nächsten Jahr in der Europäischen Union, Menschenrechtsnormen stärker zum Kern von diesen Abkommen zu machen und auch nicht mehr davon sprechen zu müssen, ob das jetzt eine zivile oder militärische Technologie ist, sondern zivil-militärisch oder auch eine Technologie die für Menschenrechtsschäden genutzt werden kann. Das ist ein wichtiger Unterschied, der zwar bisher immer mitgedacht wird in den verschiedenen bestehenden Regimen, aber nicht explizit tief in diesen Regimen verankert ist. Und deswegen ist der Vorschlag zur GiM Security von der Europäischen Kommission erst mal zu begrüßen. Gleichzeitig ist es natürlich so, dass wir alle Erkenntnisse, die wir in diesem Bereich haben, vor allen aus Quellen von investigativen Journalisten, Nichtregierungsorganisationen und forschenden Wissenschaftlern gezogen haben. Es kann nicht sein, dass wir in einem Bereich, wo es eigentlich mehr Expertise bedarf, viel zu wenig Transparenz haben. Ich habe dabei explizit das Beispiel Finnland genannt. Ich frage seit Jahren bei dem Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) nach, welche Exporte genannt werden und welche Exporte denn auch genehmigt werden und es ist relativ schwer diese Daten herauszufinden. Es braucht eine Kleine Anfrage dieses Parlaments, um überhaupt an diese Daten heranzukommen. Gleichzeitig ist es so, dass, wenn man die finnische Exportkontrollbehörde fragt und einfach nur eine E-Mail hinschickt, man in relativ kurzer Zeit eine Liste von allen Genehmigungen im letzten Jahr zugeschickt bekommt. Ähnliche Transparenz würde ich mir auch von anderen EU-Staaten wünschen. Es ist jetzt nicht so, dass Finnland nicht auch in diesem Bereich ähnliche Fragen zu klären hätte. Ich glaube, das ist das vielleicht entscheidende Argument. Es gibt viele Debatten, wie man jetzt weiter verfährt, im Bereich Exportkontrolle von Überwachungstechnologien und ich glaube da ist es wichtig, das Ziel bei dem ganzen Thema nicht aus den Augen zu lassen. Wir sind an einem Punkt, wo in den letzten Jahren relativ viel passiert ist und wo es weiterhin möglich ist über diese Regulierung sicherzustellen, dass europäische Technologien nicht für Menschenrechtsverletzungen missbraucht werden. Das kann man auch weiterhin mit entsprechenden Nachbesserungen und Veränderungen tun. Die Frage ist letztlich eher eine von effektiverer Regulierung und weniger, ob man das jetzt machen soll oder

nicht. Vielen Dank.

Der **Vorsitzende:** Vielen Dank, Herr Dr. Wagner. Und jetzt hat Herr Christian Mihr als Letzter das Wort für sein Statement, bitte schön.

SV **Christian Mihr**: Vielen Dank. Im Rahmen der Nothilfearbeit unterstützt Reporter ohne Grenzen weltweit jedes Jahr rund 600 Einzelfälle. Dabei zeigt sich, dass heute eigentlich jeder Journalist, den wir unterstützen und auch die Bürgerjournalisten zumeist in Teilen digital arbeiten und sei es, dass sie nur E-Mails schreiben. Mindestens die Hälfte der von uns jedes Jahr weltweit unterstützten rund 600 Journalisten sind in Folge von Überwachung durch Staaten oder immer mehr durch private Gewaltakteure, wie dem Islamischen Staat, sowie aus Mangel an Ende-zu-Ende-Verschlüsselung in bedrohliche Situationen geraten. Da haben wir letztes Jahr mal eine Auswertung unserer ganzen Nothilfefälle gemacht. Sie erlitten infolge von Überwachung gezielte Angriffe und Gewalt, wurden zu Unrecht inhaftiert oder mussten ihre Länder verlassen. Fest steht, etwa fünfzehn Firmen sind weltweit in dem besonders heiklen Geschäft mit Trojanersoftware aktiv, darunter die Firmen FinFisher und trovicor aus München oder die Firma Hacking Team aus Italien, die Reporter ohne Grenzen bereits 2013 als Feinde des Internets benannt hat. Eine signifikante Anzahl von Mitarbeitern wird in Deutschland nicht beschäftigt. Trovicor gilt in Deutschland als eines der größten Unternehmen in diesem Bereich und beschäftigt als solches rund 170 feste sowie eine unbekannte Zahl freier Mitarbeiter. Andere Firmen wie FinFisher beschäftigen in der Regel weniger als 100 Mitarbeiter. Derzeitige Exportkontrollregime sehen eine Vorabprüfung entsprechend der durch die exportierenden Unternehmen eingereichten Unterlagen vor. Anonym in diesem und im vergangenen Jahr auf zwei Twitterkonten veröffentlichte Leaks interner Dokumente der Firmen Hacking Team und FinFisher, früher Gamma International, zeigen jedoch, dass Verkäufe in der Regel über eine oder sogar mehrere Tochter- und Vermittlerfirmen abgewickelt werden. Nötig ist daher eine explizite und auch verpflichtende Endverwenderkontrolle. Die bisherigen internen Regelungen der Firmen sind definitiv nicht ausreichend. Das haben vor allem auch die von Reporter ohne Grenzen unter anderem gemeinsam mit dem European Center for Constitutional and Human Rights und Privacy International angestrengten OECD-Beschwerden gegen die deutsche Firma trovicor und auch gegen die deutsch-britische Firma Gamma International gezeigt. Die Effektivität des derzeitigen Kontrollregimes lässt sich, wenn man das ernsthaft bewerten möchte, im Moment noch schwer abschätzen. Einerseits ist die Implementierung des Wassenaar-Arrangements wirklich noch recht jung, bislang ist noch kein ganzes Jahr vergangen, andererseits liegen keine umfassenden Zahlen zu Ablehnungen und Annahmen von Exportanträgen vor. Außerdem wurden bislang nicht in allen Ländern des Wassenaar-Abkommens die Regelungen implementiert, darunter die USA und Russland und beide sind sehr aktiv in der Produktion solcher Technik. Der Export europäischer Software nach dem Jahr 2013 ist zumindest für das Unternehmen Hacking Team durch die schon erwähnten zugänglichen Leaks eindeutig belegt. Demzufolge lieferte Hacking Team nach 2013 Überwachungstechnologie nach Uganda. Reporter ohne Grenzen liegen zudem bislang nicht veröffentlichte, stichhaltige Hinweise auf den Export von Monitoring Centers nach 2013 durch das deutsche Unternehmen ATIS nach Ägypten vor. Letztlich sind aber nicht die Exporte nach 2013 entscheidend, um die Wirkung der Exportkontrollregulierung durch das Wassenaar-Arrangement zu beurteilen. Erst mit dem begrüßenswerten Beschluss der neuen Dual-Use-Richtlinie sind die Regeln in Europa verbindlich geworden. Um die Effektivität zu überprüfen, müssten wir also Einblick in die Dual-Use-Statistik von 2015 haben. Überarbeitungsbedarf sehen wir bei der fortwährenden Kontrolle bestimmter Verschlüsselungstechnologien. Aufgrund der mittlerweile in vielen Produkten standardmäßig eingesetzten Verschlüsselung und der deutlich fordernden Sicherheitsumgebung, Geheimdienste und IT-Kriminalität, sind diese Regelungen schlicht überholt und sollten deshalb einfach ersatzlos gestrichen werden. Bereits heute sind Forschungsergebnisse, Open Sources Software und öffentliche, für Privatanwender erwerbbare Computersoftware von den Regelungen des Wassenaar-Abkommens ausgenommen und wir erkennen aus unserer praktischen Arbeit bislang keine negativen Auswirkungen auf die Verfügbarkeit von entsprechenden Angeboten für Journalisten und Menschenrechtsver-

teidiger. Die allermeisten IT-Firmen liefern ohnehin nur an Regierungsakteure. Bei IT-Produkten liegt deshalb der Unterschied zwischen legitimer und illegitimer Nutzung nicht in der Frage, ob die IT-Güter militärisch oder zivil genutzt werden im Vergleich zu anderen Dual-Use-Produkten. Die Frage ist vielmehr, ob ein Land über einen geeigneten Rechtsrahmen verfügt, der die Verwendung solcher Güter sinnvoll beschränkt. Ich will noch abschließend ein paar Dinge zur aktiven deutschen Unterstützung sagen. Eigene Recherchen von Reporter ohne Grenzen haben die Vergabe von Hermesbürgschaften durch die Bundesregierung für den Verkauf von Überwachungstechnologien in verschiedenen Ländern belegt. Die wurden auch von Recherchen vor allen Dingen von NDR und Süddeutscher Zeitung belegt und es gab auch hier im Haus erfreulicherweise mehrere Kleine Anfragen, die weitere Hermesbürgschaften belegen. Reporter ohne Grenzen hat überdies bislang noch nicht veröffentlichte Hinweise darauf, dass die Bundesregierung Hermesbürgschaften für den Export deutscher Überwachungstechnologien vor Ausbruch des Krieges auch nach Syrien vergeben haben könnte. Öffentlich bekannt ist bereits, dass die Firma trovicor dort Anlagen installiert und gewartet hat. Dabei will ich es erstmal belassen und freue mich auch noch darauf auf weitere Aspekte, die in der schriftlichen Stellungnahme ausführlicher ausgearbeitet sind, einzugehen.

Der **Vorsitzende:** Vielen Dank an die Sachverständigen für die Eingangsstatements. Ich eröffne die Aussprache, will aber auch noch einmal darauf hinweisen, dass diese äußerst dekorative Uhr mitläuft. Man sollte darauf achten, wenn die Zeit zu Ende ist und von grün auf rot schlägt und dann auch dieses zarte Signal ertönt, dass dann die Zeit um ist. Das gilt sowohl für die Abgeordneten als auch für die Sachverständigen. Ich eröffne die Aussprache und gebe als erstes das Wort Herrn Marian Wendt von der CDU/CSU-Fraktion, bitte schön.

Abg. Marian Wendt (CDU/CSU): Vielen Dank, Herr Vorsitzender, meine Herren Sachverständige. Vielen Dank für Ihr Kommen, auch für dieses wichtige Thema und Ihre Stellungnahmen. Ich glaube, dass es schon wichtig ist, dass wir uns über das Thema in aller Sensibilität unterhalten. Es gibt da verschiedene Facetten, die wir da im Blick haben müssen und deswegen danke ich auch für Ihren sehr weiten Blick, den Sie uns hier mit Ihren Stellungnahmen eröffnet haben. Ich habe zwei Fragen an Herrn Prof. Dr. Waidner. Es ist auch in den Stellungnahmen zu lesen und es wurde auch angesprochen, dass das Thema Digital Diplomacy im Auswärtigen Amt an Stellenwert verloren hat und deswegen die Frage: Wie könnte die Wichtigkeit des Themas im Hinblick auf die Proliferation von Überwachungstechnologien und freien Netzen aus Ihrer Sicht wieder hergestellt werden? Und die zweite Frage ist sicherlich auch eine Grundfrage bevor man mit Forschungen beginnt: Wie bewerten Sie grundsätzlich den Zielkonflikt, der zwischen den berechtigten Sicherheitsinteressen des Staates und Maßnahmen der Verschlüsselung im Verhältnis zum Persönlichkeitsrecht steht. Also Sicherheitsinteressen auf der einen Seite, Möglichkeiten der Verschlüsselung von persönlichen Daten auf der anderen Seite. Das sind meine beiden Fragen, vielen Dank.

Der **Vorsitzende:** Vielen Dank, als nächstes hat das Wort Frau Wawzyniak von der Fraktion DIE LINKE.

Abg. Halina Wawzyniak (DIE LINKE.): Ich würde gerne den Versuch unternehmen, das, was ich an Interessantem erfahren habe, zumindest für mich zielführend zusammen zu führen. Deswegen werden es auch nur zwei Fragen, die sich aber trotzdem an unterschiedliche Personen richten. Ich würde darum bitten dies ausnahmsweise einmal zuzulassen, weil es ansonsten schwierig ist, zielführende Sachen zu erreichen. Ich würde gerne Herrn Dr. Gaycken und Herrn Dr. Wagner zu dem Vorschlag von Herrn Prof. Dr. Waidner fragen, ob Digital Rights Management für E- und IKT-Güter mit Dual-Use-Charakter aus Ihrer Sicht etwas sinnvolles sein kann und umgedreht Herrn Dr. Gaycken und Herrn Prof. Dr. Waidner zum Vorschlag von Herrn Dr. Wagner fragen, ob die Vorschriften zu Kryptographie und Exportkontrolle von kryptographischen Sachen gelockert werden können. Ich weiß, dass das eigentlich gegen die Regeln ist, aber es ist sonst schwierig in dieser Anhörung, zumindest für mich, etwas herauszubekommen, was ich dann auch politisch verwenden kann.

Der **Vorsitzende:** Da Sie immer so sparsam mit der

Zeit sind, darf es so sein. Jetzt hat als nächstes das Wort Herr Reichenbach und dann Herr Klingbeil, die sich die Fragen teilen, bitte schön.

Abg. Gerold Reichenbach (SPD): Gut, dann fange ich einmal an. Ich habe eine Frage an Herrn Prof. Dr. Waidner und zwar bezieht sich das auf Ihren Leitgedanken 7. Also die Idee ist zunächst einmal faszinierend für mich, zu sagen, man kann eher solche Software auch von der Fahne über das Internet kontrollieren und entsprechend auch bestimmte Dinge abschalten. Meine Frage ist allerdings, wenn wir es ja bei Software noch viel stärker mit dem Dual-Use-Gedanken zu tun haben, das heißt also, dass ich sie in unterschiedlichen Situationen völlig unterschiedlich benutzen kann, auch als Überwachungssoftware, wie soll das erkannt werden? Sonst greift das Instrument ja nur sehr beschränkt.

Der **Vorsitzende:** Herr Klingbeil, bitte.

Abg. Lars Klingbeil (SPD): Meine Frage geht an Herrn Dr. Gaycken. Ich habe in Ihrer schriftlichen Stellungnahme eine Sache gelesen, über die ich dann doch gestolpert bin, wo ich einfach einmal nachfragen will. Sie haben in der Antwort zu Frage 8 das Unternehmen Palantir und deren Rolle angesprochen und das dann auch in Zusammenhang gebracht mit dem designierten Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik und sind am Ende zu der Schlussfolgerung gekommen, dass eine Einbindung des Bundesamtes für Sicherheit in der Informationstechnik in die Exportkontrollen zukünftig politisch schwierig wird. Und da bin ich an der Stelle wach geworden und hätte gerne noch einmal ein paar ausführliche Informationen von Ihnen dazu.

Abg. Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Das würde mich in der Tat auch interessieren. Dazu zwei Fragen ergänzend. Die erste an Herrn Mihr. Ich habe das eben so wahrgenommen, dass Sie auf einen konkreten Fall Bezug genommen haben. Entschuldigen Sie, dass ich Ihnen so in den Rücken sprechen muss. In Ihrer Stellungnahme beschreiben Sie, dass Sie Hinweise darauf haben, dass die Bundesregierung den Export von Überwachungs- und Spionagesoftware nach Ägypten und Syrien unterstützt hat. Ich zitiere aus Ihrer Stellungnahme: „*Reporter ohne Grenzen liegen zudem bislang nicht veröffentlichte, stichhaltige Hinweise auf den Export von Monitoring Centern nach 2013 durch das deutsche Unternehmen Atys nach Ägypten sowie in andere Länder mit einer gleichfalls problematischen Menschenrechtssituation vor. Reporter ohne Grenzen hat überdies bislang noch nicht veröffentlichte Hinweise darauf, dass die Bundesregierung Hermesbürgschaften für den Export deutscher Überwachungstechnologien vor Ausbruch des Krieges auch nach Syrien vergeben haben könnte. Öffentlich bekannt ist bereits, dass die Firma Trovicor dort Anlagen installiert und gewartet hat.*“ Das wäre in der Tat ein gravierender und interessanter Fall. Vielleicht gibt es da einen aktuellen Stand, der würde mich sehr interessieren. Und die zweite Frage, vielleicht einfach an Herrn Prof. Dr. Waidner: Das Problem, das wir hier diskutieren, ist Jahre alt. Wir diskutieren das seit Jahren, die Problematik war altbekannt, die Fälle, Herr Mihr hat sie aufgezählt, die kennt man. Was hat die Bundesregierung eigentlich die letzten Jahre gemacht? Also ich kann mich erinnern, wir haben hier einen Gesetzesentwurf 2013 vor der Bundestagswahl diskutiert, der kam leider von der Opposition und nicht von der Bundesregierung und dann gab es irgendwie im Wirtschaftsministerium mal so eine Andeutung, dass man das Thema interessant findet, aber gibt es irgendetwas Konkretes, was passiert ist? Vielen Dank.

Der **Vorsitzende:** Herr Prof. Waidner für die Frage vom Abgeordneten Wendt.

SV **Prof. Dr. Michael Waidner**: Also es waren ja zwei Fragen. Was ich gerne beantworte ist die Frage zur Verschlüsselung und dem möglichen Zielkonflikt, den es geben könnte. Es ist völlig unbestritten natürlich, dass in manchen Fällen Verschlüsselung, Strafverfolgung und ähnliche Dinge vermieden und dementsprechend es nützlich wäre und ist, verschlüsselte Nachrichten lesen zu können. Jetzt muss man einfach überlegen, dass es mehrere Möglichkeiten gibt, wie man das erreichen kann. Verschlüsselung kann man versuchen zu brechen, indem man Fehler findet, indem man die Algorithmen versucht zu knacken usw. Es ist unbestritten, dass jeder so etwas versucht oder gar absichtlich Hintertüren einbaut, die den ganzen Zweck konterkarieren. Also Verschlüsseltes muss erst einmal sicher sein. Hintertüren könnten von

anderen gefunden werden, die könnten aufgedeckt werden, die könnten auch auf einmal einen blank dastehen lassen. Deswegen ist es wichtig, dass Kryptographie an sich erst einmal sicher ist. Es gibt natürlich immer die Möglichkeit, statt die Kryptographie, die Implementierung oder die Endpunkte anzugreifen und dann eben wie bei der Quellenüberwachung an den Quellen solche Dinge zu machen. Jetzt für die Exportkontrolle ist mein Plädoyer an und für sich zu sagen, der Schutzgedanke muss im Vordergrund stehen. Aus diesem Grunde plädiere ich dafür zu sagen, starke Kryptographie muss komplett aus jeder Exportrestriktion herausgenommen werden. Wichtig ist, dass der Breitenschutz im Vordergrund steht. Der Breitenschutz kann nur dann funktionieren, wenn die Kryptographie wirklich sicher ist. Es ist mein Versuch zu antworten. Ich hoffe es hat ungefähr das getroffen, was Sie wissen wollten.

Abg. Marian Wendt (CDU/CSU): Die Sicherheitsinteressen eher in den Vordergrund als die individuellen Persönlichkeitsrechte zu stellen. Auf so einer Skala sage ich, versuchen wir uns auch immer graphisch einzuordnen.

SV **Prof. Dr. Michael Waidner**: Also ich würde sagen, die Sicherheit der Einzelnen muss gegenüber dem staatlichen Interesse im Vordergrund stehen an dieser Stelle, Einzelne überwachen zu können oder gar dem Interesse, welches niemand haben sollte, Massenüberwachung zu betreiben. Gut, Ihre andere Frage ging, glaube ich, in Wirklichkeit nicht an mich, sondern an Herrn Dr. Gaycken, der dafür plädiert hat, im Auswärtigen Amt mehr Serversicherheit unterzubringen.

Der **Vorsitzende:** Die Worterteilung mache ich dann schon. Vielen Dank erst einmal. Nun zur Antwort auf die Frage von Frau Wawzyniak, Herr Dr. Gaycken und Herr Dr. Wagner wurden benannt. Sie bekommen jeweils drei Minuten, die Sie sich bitte teilen. Und anschließend Herr Prof. Dr. Waidner und Herr Dr. Wagner, Sie haben dann auch drei Minuten. Also erstes Herr Dr. Gaycken und Herr Dr. Wagner, die erste Frage von Frau Wawzyniak, bitte schön.

SV **Dr. Sandro Gaycken:** Kurz zu den beiden Fragen. Das Digital Rights Management für IKT mit Dual-Use ist mäßig sinnvoll. Man kann damit natürlich nur versuchen die Weiterverbreitung zu verhindern. Es kann allerdings in den Kontexten auch viel umgangen werden, zumindest gibt es keine Digital Rights Management-Technologien, die wirklich hundert Prozent sicher sind. Davon abgesehen sind natürlich viele der Dual-Use-Technologien schwierig zu bewerten, wenn diese verkauft werden. Bei Lawful Interception-Technologien aus dem Westen kann man die Skalierung und auch diese Codewörter schlecht begrenzen. Von daher kann man auch gar nicht garantieren, dass die dann nicht doch in autoritäre Kontexte geraten und autoritär genutzt werden. Das größere Problem ist aber, wie ich in meiner Stellungnahme auch gesagt hatte, dass viele der Dual-Use-Technologien gar nicht als solche erscheinen. Vor allem die Big Data-Analysen, wie von der Firma Palantir, die im Moment sehr intensiv für Überwachungszwecke in vielen Ländern genutzt werden, spielen eine Rolle. Diese sind gar nicht auf dem Radar für die meisten Sachen. Noch zu der anderen Frage, ob für kryptographische Anwendungen und Forschung die Regelungen gelockert werden können. Das ist schwierig zu beurteilen. Das ist schlicht und ergreifend das Interesse der internationalen Sicherheitspolitik. Da sind dann eben der Iran und der Islamische Staat auch nicht mehr zu hacken. Und da kann man dann auch nicht mehr in andere Computersysteme hineinschauen. Eine ellenlange Diskussion, die wir schon seit Jahrzehnten haben, ob wir das machen sollen oder nicht. Von daher würde ich aber nicht für eine Lockerung plädieren, sondern für eine kontrollierte Ausgabe und einen kontrollierten Umgang damit, weil die Gefahr doch zu hoch ist, dass man sehr gefährlichen Akteuren damit eine sehr hohe Abschirmung gibt.

Der **Vorsitzende:** Herr Dr. Wagner, bitte.

SV **Dr. Ben Wagner**: Ich versuche das in eineinhalb Minuten, schnell abzuschließen. Es gibt Beispiele, die bekannt sind zum Beispiel aus Tunesien, wo tatsächlich solche Software abgeschaltet worden ist auf Grundlage von solcher Technologie. Aber da geht es meistens nicht um Menschenrechtsverletzungen, sondern schlicht und ergreifend darum, dass nicht gezahlt wurde. Man muss sich das nicht als Software, sondern als Dienstleistungsgesamtpaket vorstellen, das geliefert

wird. Wenn man dann merkt, dass nicht bezahlt wird oder irgendwas nicht gemacht wird, was dem Hersteller nicht passt, bestehen Möglichkeiten, die auch eingesetzt werden können. Die Gefahr dabei ist, dass man die bestehende Kontrolle dagegen ausspielt und sagt, wenn man jetzt solche Möglichkeiten hat, reicht es dann auch und das ist dann gleich eine Endverbleibskontrolle oder derartiges. Das eine gegen das andere auszuspielen ist, glaube ich, nicht sinnvoll. Es braucht sowohl die Endverbleibskontrolle als auch die technischen Möglichkeiten, die auch entsprechend von den Firmen genutzt werden. Das ist aber bisher vielfach nicht der Fall. Da gibt es mehr technische Möglichkeiten, als man bereit wäre zuzugeben, gerade weil meistens so ein Gesamtpaket geliefert wird.

Der **Vorsitzende:** Vielen Dank. Und auf diese Frage antworten jetzt Herr Prof. Dr. Waidner und dann Herr Wagner. Herr Prof. Dr. Waidner, bitte schön.

SV **Prof. Dr. Michael Waidner**: Das war jetzt die Frage zur Kryptographie, nicht wahr? Wie eben schon gesagt, ich würde dafür plädieren, Kryptographie nicht nur zu lockern, sondern tatsächlich komplett aufzugeben, also auch nicht zu limitieren, wie Herr Dr. Gaycken das vorschlägt, sondern komplett frei zu geben. Das hat an und für sich zwei Gründe. Einen habe ich schon gesagt, Kryptographie ist eine Grundmethode des Schutzes und der Schutz muss Vorrang haben. Das andere ist, man muss sich im Klaren darüber sein, dass Kryptographie etwas ist, das kompliziert klingt aber nicht ist. Das heißt, man hat durch Exportkontrollen an dieser Stelle so gut wie keine Chance. Die meisten kryptographischen Softwareimplementierungen sind Open Source. Selbst kommerzielle Implementierungen, die man für viel Geld von großen Herstellern kauft, sind real gesehen nur blau, grün, rot gewaschene Open Source-Implementierungen. Das heißt, man kann das überhaupt nicht kontrollieren, man verliert nichts und man gewinnt einfach nur, dass man in beliebigen Ländern sichere Kommunikation auch für Regimegegner und für unterdrückte Bevölkerungsgruppen hinbekommt.

Der **Vorsitzende:** Herr Dr. Wagner, bitte.

SV **Dr. Ben Wagner**: Ganz kurz dazu. Ich glaube, ich kann das auch so unterschreiben, wie Herr Prof. Dr. Waidner das gesagt hat. Ich denke, es ist sinnvoll, das so zu sehen. Ich würde vielleicht noch ergänzen, dass es bei der derzeitigen Kontrolle bereits auch so schon für größere staatliche oder mit viel Geld ausgestattete Akteure möglich ist, dass sie sich diese Technologie zulegen. Das heißt im Prinzip, es führt im Moment dazu, wenn man eine solche Kontrolle über Kryptographie, wie sie derzeit existiert, durchführt, dass vor allem den kleinen Akteuren, die man eigentlich gerne schützen würde, die Möglichkeit, Zugang zu diesen Technologien zu bekommen, entzieht. Ich würde dabei auch nochmals betonen, namenhafte, große europäische Industrieakteure plädieren auch dafür, Kryptographie zu lockern. Also es ist nicht nur eine Forderung von Informatikern oder Wissenschaftlern oder aus der Zivilgesellschaft, sondern auch die Industrie hätte gerne eine Lockerung von diesen Vorschriften. Letztlich weil das eine so übliche Komponente in diversen Arten von Software ist, dass es fraglich ist, warum es überhaupt in dieser Form in der bestehenden Regulierung existiert.

Der **Vorsitzende:** Herr Prof. Waidner für die Frage von Herrn Reichenbach.

SV **Prof. Dr. Michael Waidner**: Das war jetzt gerade die Frage, wie Digital Rights Management in diesem Zusammenhang funktionieren könnte. Zunächst einmal möchte ich sagen, es soll kein Allheilmittel sein. Ich habe nur überlegt, was könnte man technisch überhaupt tun. Wie wir gerade schon gehört haben, gibt es Möglichkeiten, dass man durch Digital Rights Management, also durch das nachträgliche Abschalten von Funktionalitäten, gefährliche Produkte schlicht abschalten kann. Diesen Digital Rights Management-Kopierschutz kann man umgehen, typischerweise technisch, was Herr Dr. Gaycken freundlich angedeutet hat. Das ist sicherlich richtig. An dieser Stelle ist es so: Glaubt man den Hochtechnologieländern, in die man exportiert, dann brauchen sie uns nicht. Oder glaubt man sie sind von uns technisch gesehen abhängig, dann kann so etwas auch gegen Unterdrücker helfen. Es hilft sicherlich nicht gegen beliebige Überwachungssoftware, sondern nur gegen explizite Software, die zum Überwachen da ist. Wir nehmen jetzt an, dass Exploits

unter Exportkontrolle gestellt werden. Natürlich kann man die Exploits nicht abschalten durch so etwas, das wäre naiv anzunehmen. Ich denke letztlich, Digital Rights Management ist eine Methode, die oft, aber nicht immer hilft. Sie kann sicherlich manchmal umgangen werden, aber sie ist besser als nichts.

Der **Vorsitzende:** Herr Klingbeil hat den Sachverständigen Herrn Dr. Gaycken gefragt, bitte schön.

SV **Dr. Sandro Gaycken:** Die Frage der Abgeordneten war, glaube ich, ob mir Kontexte bekannt sind zwischen Überwachungsfirmen, kontroversen Firmen und Bundesstellen. Diesbezüglich ist mir jetzt leider eingefallen, dass Arne Schönbohm, der jetzt designierte Präsident des Bundesamts für Sicherheit in der Informationstechnik, vorher den Lobbyverband Cyber-Sicherheitsrat Deutschland e. V. geleitet hat. In diesem Lobbyverband hat er versucht IT-Sicherheitsfirmen, in den deutschen Markt hineinzubringen. Dazu gehörten leider auch die beiden Firmen Palantir und Blue Code. Blue Code ist eine Firma, die bekannt dafür war, dass sie schon Überwachungstechnologien an den Iran, Syrien, den Sudan und nach China verkauft hat, womit Oppositionelle verfolgt wurden. Palantir ist eine der schlimmsten Big Data-Analysten, welche von der CIA gegründet und großgezogen wurden. Sie wurden benutzt, um alle möglichen Profile anzulegen und zu verkaufen. Sie versuchen jetzt auch in den Emiraten und in Europa Sachen zu verkaufen. Sie haben also sehr starken Dual-Use-Charakter. Weiterhin kann man sie auch benutzen, um Business Daten zu analysieren. Zu bedenken ist aber, dass sie stark aus der Intelligence-Ecke kommen und sehr kontroverse Sachen machen. Abgesehen davon ist Schönbohm jetzt kompetent. Ob er aber ausgerechnet mit diesem Hintergrund Präsident des Bundesamts für Sicherheit in der Informationstechnik werden sollte, scheint mir politisch schwierig, wo er doch die Sorgen in der deutschen Wirtschaft an das Bundesamt für Sicherheit in der Informationstechnik weiterleiten soll und gerade vor diesen Firmen warnen sollte.

Der **Vorsitzende:** Herr Mihr und Herr Prof. Waidner, Sie beantworten jetzt bitte die Fragen von Herrn Dr. von Notz.

SV **Christian Mihr**: Ich muss jetzt auch mit dem Rücken reden, das ist einfacher, weil mir ja schon mit dem Rücken zugeredet wird. Es ging einerseits um die Frage nach den Hermesbürgschaften und andererseits nach den Exporten. Es ist tatsächlich so, dass wir stichhaltige Informationen zugespielt bekommen haben, dass 2013 durch das deutsche Unternehmen ATIS Monitoring Center, welche technisch die Überwachung von Internetströmen ermöglichen, nach Ägypten geliefert wurden. Diesbezüglich haben wir auch schriftlich vorliegende Informationen, welche noch nicht veröffentlicht wurden. Allerdings kann ich schon ankündigen, dass im Januar ein Bericht von Privacy International geplant ist, zu dem wir Teile beigesteuert haben. Auch wenn ich etwas früher bereits gesagt habe, dass die Exporte nach 2013 für die Frage der Effektivität des Kontrollregimes gar nicht so aussagekräftig sind, ist es trotzdem ein Skandal, wenn das 2013 passiert ist und wir auch dafür diese sehr stichhaltigen Hinweise haben. Bezüglich der Frage der Hermesbürgschaften, habe ich erwähnt, dass wir auch dort noch nicht veröffentlichte, sehr plausibel erscheinende Hinweise haben, dass es offenbar in den 2000er Jahren Hermesbürgschaften für den Export nach Syrien gegeben haben könnte. Diese erscheinen uns deshalb plausibel, da sie aus einer Quelle stammen, die dort sehr nahe gewesen ist. Zum einen ist bekannt, dass Monitoring Center und Software nach Syrien geliefert wurden und zweitens, dass diese Technik auch nicht umsonst in das Sanktionsregime aufgenommen wurde. Insofern verstehe ich die Erwähnung dieses Hinweises eher als eine Ermutigung, eine Aufforderung oder einen Wunsch auch an das Parlament, in Form einer kleinen Anfrage etc. mehr darüber herauszufinden. Die meisten Erkenntnisse, die wir zu dem Stichwort Hermesbürgschaften haben, basieren entweder auf journalistischen Recherchen, Organisationsrecherchen oder kleinen Anfragen. Insofern ist das ein Wunsch und eine Aufforderung an dieses Parlament diesen Fragen in irgendeiner Form noch einmal explizit nachzugehen. Denn uns erscheint dieser Hinweis in dem Gesamtkontext auch von der Quelle, die ich hier nicht nennen kann, sehr plausibel.

Der **Vorsitzende:** Herr Prof. Waidner, bitte.

SV **Prof. Dr. Michael Waidner**: Die Frage war

glaube ich, wie man das bewertet oder was die Bundesregierung bisher getan hat. Und da ich nicht die Bundesregierung bin, fällt es mir etwas schwer, das zu beantworten. Was ich sagen kann ist, dass meinem Verständnis nach die Bundesregierung hinter den Prinzipien, die wir hier alle gerade vertreten haben, steht. Also scheint die Entwicklung durchaus positiv zu sein. Was die Bewertung betrifft, erteile ich zwar nicht das Wort, aber würde gerne die Gelegenheit dazu nutzen, die Frage einfach weiterzugeben, da sie von Herrn von Notz an alle gerichtet war.

Der **Vorsitzende:** Wir machen in der Ordnung weiter, wie wir es gewohnt sind. Ich komme zur offenen Fragerunde. Jetzt kann gerne alles noch benannt und besprochen werden, das machen wir dann face to face. Als erste hat das Wort Frau Wawzyniak, dann Herr Janecek, dann Herr Schipanski und dann sehen wir weiter. Bitte schön.

Abg. Halina Wawzyniak (DIE LINKE.): Diesmal ist es ganz einfach, obwohl es nach demselben System wie vorhin funktioniert. Diesmal beziehe ich mich auf etwas, was Herr Mihr gesagt hat. Er hat nämlich gesagt, dass die Endverbraucher- oder Endverwenderkontrolle zentral sein sollte. Zur Frage Endverwenderkontrolle hätte ich gerne die Meinung von Herrn Dr. Wagner und Herrn Dr. Gaycken.

Der **Vorsitzende:** Bitte schön, Sie teilen sich die Zeit.

SV **Dr. Ben Wagner**: Die Qualität der Endverwenderkontrolle ist natürlich nicht nur im Bereich Überwachungstechnologien, sondern grundsätzlich im Bereich von Exportkontrolle gelegentlich etwas bescheiden, um es einmal vorsichtig auszudrücken. Da gibt es viel Spielraum und viel Bedarf zur Verbesserung. Die Schwierigkeit ist natürlich, wie man so eine Kontrolle im Ausland im Kontext zu bestehenden Regelungen überhaupt sinnvoll schaffen kann. Da ist viel Luft nach oben und es gibt verschiedene Möglichkeiten. Diese werden vor allem derzeit im Rahmen der neuen EU-Dual-Use-Verordnung diskutiert. Dort ist der Ort, wenn man sinnvolle Vorschläge hat, um die entsprechende Endverwenderkontrolle zu verbessern. Ich glaube, das Schwierige dabei ist immer, dass daraus dann geschlossen wird, dass diese Exportkontrollen gar nicht nützlich sind, wenn man gar nicht kontrollieren kann und sich die Frage stellt, warum man sie überhaupt benutzt. Und ich glaube, dass man auch trotz imperfekter Umsetzung der Endverwenderkontrolle von einer Gesamtsinnhaftigkeit des Prozesses sprechen kann. Das rührt daher, dass das System an sich dazu führt, dass weniger derartiger Technologien exportiert werden, was man auch immer wieder bei den einzelnen beteiligten Firmen sieht. Auch wenn das bei Leibe kein perfektes System ist.

Der **Vorsitzende:** Herr Dr. Gaycken bitte.

SV **Dr. Sandro Gaycken:** Ich kann mich dem eigentlich nur anschließen. Es ist ja in der Tat sehr schwierig, das im einzelnen Gebrauchskontext zu sehen. Es sind Dinge, die sehr stark abgeschlossen in Bereichen passieren, an die man gar nicht herankommt und die man gar nicht richtig sehen kann. Das kann, muss aber nicht so stark nach außen dringen, was da passiert. Das kann sehr tief eingegraben irgendwo in diesem System sein, in irgendwelchen streng geheimen Abteilungen. Von daher ist es doch sehr schwierig, in diese Kontexte hineinzukommen. Was natürlich nicht bedeutet, dies gebe mir ein Recht, aufzugeben und gleich das Handtuch zu werfen. Man muss sich überlegen, wie man vielleicht auch in diese Geheimbereiche mit irgendwelchen Kontrollregimen hineinkommt, um dann zu sehen, wie die realen Ausdehnungen sind.

Der **Vorsitzende:** Kollege Janecek, bitte schön.

Abg. Dieter Janecek (BÜNDNIS 90/DIE GRÜNEN): Vielleicht eine Information zum Thema Hermesbürgschaften. Wir haben in der letzten Legislaturperiode entsprechend abgefragt, die Informationen waren dann auch für Abgeordnete einsehbar und wir haben das Ganze entsprechend auch mit einem Antrag unterlegt. Da bleiben wir auch sicher daran und das ist auch notwendig. Vielleicht noch eine grundsätzliche Aussage. Ich bin auch Mitglied des Wirtschaftsausschusses. Unsere Reisetätigkeit ist momentan sehr stark in Krisenregionen ausgeprägt. Wir waren in der Golfregion. Russland soll jetzt drankommen und war auch schon zum Teil dran. Das ist ein Fokus, der stattfindet und

wir schauen auch ganz genau hin, was das bedeutet und ob da die Menschenrechte nicht auch unter die Räder geraten. Das ist zum Teil mein Verdacht, muss ich ehrlich sagen, wenn ich manche Stellungnahmen und auch Bemühungen in dem Kontext sehe. Ganz konkrete Frage an Herrn Mihr: Wir hatten ja auch im Vorfeld von Saudi Arabien schon einmal Kontakt. Das soll jetzt nicht speziell der Fokus sein, sondern, ob Sie noch einmal aufzählen können, anhand konkreter und belegter Einzelfälle, die Sie auch betreuen, wo Sie wirklich mit dem Thema Export und der Problematik, die dann aufgetreten ist, in Kontakt gekommen sind, um das einmal anschaulich zu machen. Danke.

Der **Vorsitzende:** Herr Mihr, bitte schön.

SV **Christian Mihr**: Ich habe bereits vorhin gesagt, dass wir im vergangenen Jahr eine Auswertung von unseren 600 Nothilfefällen gemacht haben. Ich könnte jetzt über 300 Fälle referieren, was in drei Minuten sehr ehrgeizig wäre. Das mache ich lieber nicht. Ich versuche zwei oder drei aussagekräftige Fälle, die tatsächlich auch mit den Regionen zu tun haben, zu beschreiben. Ein Fall ist zum Beispiel der Fall von Said Yousif Almuhafdha. Das ist der Vizepräsident des bahrainischen Zentrums für Menschenrechte aus Bahrain, der viele Berichte von Opfern von Folter und Polizeigewalt in dem Golfstaat dokumentiert hat. Er ist mittlerweile im Exil in Berlin. Wir haben ihn bei dem Gang in das Exil unterstützt. Aber in Bahrain kamen viele ausländische Journalisten zu ihm, um mit seiner Hilfe Menschen zu treffen, die Opfer von Folter und Polizeigewalt waren. Irgendwann fiel Said Yousif Almuhafdha auf, dass die Polizei oder der Geheimdienst immer öfter schon vor ihm bei seinen Gesprächen eintrafen. Und da hat er geahnt, dass seine Telefon- und Internetkontakte überwacht wurden. Es wurden dann im Rahmen von einer forensischen Analyse tatsächlich auch Trojaner gefunden und inzwischen ist Almuhafdha mit Unterstützung des Nothilfereferates von Reporter ohne Grenzen auch nach Deutschland geflohen. Und da arbeiten wir zu diesem Themenkomplex weiter sehr eng zusammen. Der zweite Fall, den ich vielleicht erwähnen kann, berührt vor allem die Frage nach der Proliferation, die vorhin auch noch einmal von Marian Wendt angesprochen wurde. Ein aktueller Fall aus Rakka in Syrien, wo wir Medienaktivisten von einem Medienaktivistenkollektiv, nämlich Raqqa is Being Slaughtered Silently (RBSS), zum Teil auch beim Gang ins Exil unterstützen, gerade weil die Situation so bedrohlich ist, dass vor kurzem Menschen in Rakka dramatisch ermordet wurden. Von dort wissen wir, dass sie überwacht werden und deswegen die Kommunikation gerade relativ schwierig ist. Mehr kann ich dazu auch aufgrund der Brisanz nicht sagen. Ein dritter Fall ist vielleicht noch Iran. Ein interessanter Fall, der auch vor allen Dingen die Überwachung hier im Exil betrifft. Iran war vor allen Dingen nach der grünen Revolution 2009 eines jener Länder, wo wir im Rahmen der Nothilfe besonders viele Journalisten und Aktivisten nicht nur im Land unterstützen mussten, sondern tatsächlich auch bei dem Gang in das Exil. Und dort wissen wir von einigen Journalisten, die bis heute überwacht werden. Von dem vergangenen Jahr wissen wir, dass eine forensische Analyse ergab, dass Handys von Iranern, die hier sind, Trojaner gefunden wurden. Das sind drei Fälle, aber da könnte ich Dutzend erzählen.

Der **Vorsitzende:** Kollege Schipanski, bitte schön.

Abg. Tankred Schipanski (CDU/CSU): Vielen Dank, Herr Vorsitzender. Ich hätte eine Frage an Herrn Prof. Waidner. Sie arbeiten nun im Forschungsbereich bei dem Fraunhofer Institut. Wir haben jetzt auch drei IT-Sicherheitsforschungszentren eingerichtet, in Saarbrücken, in Karlsruhe und in Darmstadt. Sie haben uns vorhin erklärt, dass faktisch die Gefahr darin besteht, das Schwachstellen ausgenutzt werden und natürlich diese IT-Sicherheitsforschungseinrichtung, die jetzt frisch eingerichtet wurden und auch Ihr Institut, sicherlich daran arbeiten, diese Schwachstellen zu beseitigen oder zu identifizieren. Da würde mich nur forschungspolitisch interessieren, ob unsere Beiträge, die wir in diese Richtung tun, ausreichen und wie Ihre Erkenntnisse eigentlich entsprechend in solche Prozesse, wie wir sie heute hier besprechen, einfließen.

Der **Vorsitzende:** Herr Prof. Waidner, bitte schön.

SV **Prof. Dr. Michael Waidner**: Das Analysieren und das automatisierte Finden von Schwachstellen ist in der Tat eines der Hauptthemen in allen drei dieser von Ihnen genannten Institute. Da ist Deutschland und die deutsche Forschung, denke

ich, auch sehr führend. Ich würde nicht sagen, es reicht aus, was wir tun, aber wir tun schon relativ viel. In diesem Kontext wollte ich zwei Sachen ansprechen. Das eine ist, dass das Finden von Schwachstellen typischerweise erfordert, dass man Dinge tut wie Reverse Engineering von Software und von Hardware. Das hat jetzt weniger mit Exportkontrolle zu tun. Das sind Hemmnisse, wo ich generell dafür plädiere, Forschung müsste dort auch frei sein und man sollte Forschern die Unsicherheit nehmen, ob das, was sie tun, im rechtlichen Rahmen dessen ist, was zulässig ist. Das ist die eine Sache. Das heißt, dass alle unsere Forschung Herstellern mitgeteilt wird. Die Hersteller werden aufgefordert die entsprechenden Schwachstellen zu beseitigen. Das passiert typischerweise auch. Es ist so, dass Schwachstellen im Endeffekt zur Überwachung ausgenutzt werden können. Es gibt einen regen Handel mit Schwachstellen, an dem wir, unnötig zu sagen, natürlich in keiner Weise beteiligt sind. Aber auch da muss ich sagen, dass das beste Mittel gegen diese Art von Handel mit Schwachstellen ist, die freie Forschung zu unterstützen, Schwachstellen zu finden, diese Schwachstellen mit den Herstellern zusammen zu beheben und diesen Wettlauf zwischen denjenigen die Schwachstellen finden wollen, um angreifen zu können und denjenigen die das aus guten Gründen tun, zu Gunsten derjenigen zu entscheiden, die das aus guten Gründen tun. Vielen Dank.

Der **Vorsitzende:** Danke. Kollege Jarzombek, bitte.

Abg. Thomas Jarzombek (CDU/CSU): Ich würde gerne meine Frage an Herrn Dr. Gaycken stellen. Und zwar, wie sich rund um diesen Kontext die Frage dessen verhält, wie Anbieter mit Daten insbesondere von, wie auch immer gearteten Dissidenten oder Bürgerrechtlern in den vorhin genannten Ländern umgehen. Also wie sicher die Dinge tatsächlich sind und ob Passwörter an Regierungen verraten oder nicht verraten werden. Wie ist Ihre Erfahrung und gibt es da auch einen staatlichen Einfluss, den wir möglicherweise wahrnehmen können?

Der **Vorsitzende:** Herr Dr. Gaycken.

SV **Dr. Sandro Gaycken**: Vielen Dank für die Frage. In der Tat ist es so, dass wir relativ viele Erkenntnisse aus China haben, weil es in China schon eine relativ stark ausgebreitete und professionalisierte Struktur gibt. China hat jahrelang versucht, auch von den westlichen IT-Anbietern, immer wieder die Daten von Oppositionellen und von Bürgerrechtlern zu bekommen, um damit besser arbeiten zu können. In China gilt vor allem der Ansatz, dass man sehr stark versucht eher regulativ an Daten zu kommen als über Spionagesoftware. Das war immer viel Hin und Her. Die IT-Firmen haben sich natürlich geweigert, auch aus dem Interesse daran ihren Marktanteil weltweit nicht zu verlieren und nicht durch kontroverse Aktivitäten einzugrenzen. Wobei China aber daraufhin damit reagiert hat, dass sie ihre eigene Suchmaschine und ihre eigenen Social Media Geschichten gebaut haben. Was wir jetzt seit kurzem ebenfalls aus China hören ist, dass sie Verschlüsselungen immer wieder abschalten. Alles was nicht beherrscht wird, wird abgeschaltet. Ansonsten lässt man nur das zu, was man staatlich auch intensiv kontrollieren kann. China ist in dieser Beziehung immer ein Vorreiter, weil sie da schon weit sind. Im Iran sehen wir das auch. Man lässt nur die Anbieter zu, die kooperieren. Die anderen werden herausgeschmissen, abgeschaltet oder durch eigene Anbieter und Varianten ersetzt. Von daher ist das ein schwieriger Trend. Und dann ist es auch natürlich schwierig mit Exportkontrollen von außen heranzugehen. Von daher war auch mein Plädoyer in meiner Stellungnahme so zu verstehen, dass sich die Außenpolitik sehr viel umfangreicher mit diesem Thema befassen muss als einfach nur mit Exportkontrollen. Wenn man also wirklich möchte, dass das Internet im Iran, in China, in Russland und in anderen Ländern nicht in eine wahnsinnige Überwachungsmaschinerie umgebaut wird, dann muss man an vielen anderen Vektoren vielleicht mit vielen anderen Hebeln noch einmal arbeiten. Außen- und sicherheitspolitisch und nicht nur mit der Exportkontrolle, weil sich gerade diese Anbieterkooperation und diese Art der Industriepolitik in den Ländern dieser Kontrollen entziehen.

Der **Vorsitzende:** Herr Kollege Janecek bitte.

Abg. Dieter Janecek (BÜNDNIS 90/DIE GRÜNEN): Ich habe eher eine Erkenntnis- und Verständnisfrage. Ich weiß nicht, wer sie von Ihnen am besten

beantworten kann, aber auf EU-Ebene gibt es eine Surveillance Technology Expert Group und wir würden gerne einmal hinterfragen, was die Rolle Deutschlands dabei ist und was genau dort diskutiert wird mit welchem Ziel. Vielleicht können Sie sich einigen, wer das beantwortet, ich weiß es nicht.

Der **Vorsitzende:** Herr Dr. Wagner.

SV **Dr. Ben Wagner**: Weil das Thema so komplex ist, hat man, soweit ich das weiß, ich bin da nicht hundertprozentig sicher, auf Initiative der Bundesregierung eine solche Arbeitsgruppe eingeführt, die im Prinzip Expertise bündeln soll. Meines Wissens nach sind das sieben Mitgliedsstaaten, ich kann Ihnen gerne nochmal separat eine Liste dazu schicken, die Anhörungen und Expertise zu diesem Thema bündeln, um sicherzustellen, dass die EU auch gerade im Hinblick auf die Novellierung der Dual-Use-Richtlinie die maximale Menge an Expertise zur Verfügung hat. Soweit ich weiß, wurden dort sowohl Firmen als auch Zivilgesellschaftler gehört und eingeladen Stellung zu nehmen. Und was man zumindest mitbekommt aus der EU und auch aus dieser Arbeitsgruppe, sind sie sehr offen für die Belange, die hier diskutiert werden. Es ist zwar ein noch relativ geschlossenes Verfahren, es könnte durchaus ein bisschen transparenter sein, aber von dem, was man inhaltlich davon hört, scheint es auch im Sinne dieser Anhörung zu sein.

Der **Vorsitzende:** Vielen Dank. Gibt es weitere Wortmeldungen? Das ist offensichtlich der Fall. Kollege Janecek.

Abg. Dieter Janecek (BÜNDNIS 90/DIE GRÜNEN): Ich bin heute ganz neugierig. Ich habe noch eine Frage zum Verständnis dieser Industrie. Ich komme aus Bayern. Bayern ist ein Standort für Spionagesoftware. Vielleicht kann Herr Mihr oder vielleicht auch wieder Ihr Nachbar das noch einmal schildern Wie sieht diese Industrie aus? Man hört auch immer, dass es einen sehr schwierigen Zugang zu dieser Industrie gibt. Berichterstattung ist auch schwer möglich. Bei Kongressen werden Journalisten eher gemieden, das sind zwar Gerüchte, aber natürlich können Sie dies vielleicht auch verifizieren.

Der **Vorsitzende:** Herr Mihr.

SV **Christian Mihr**: Das Problem bei dieser ganzen Industrie ist es natürlich, dass es schon vom Selbstverständnis und vom Kern ihres Geschäfts her ein hohes Interesse an Transparenz gibt. Das ist, glaube ich, das Grundproblem und deswegen muss man auch Schätzungen, die es dazu gibt immer mit einer gewissen Vorsicht genießen. Aber vielleicht um einmal ein paar Zahlen zu sagen. Es gibt durchaus Schätzungen zum globalen und weltweiten Marktvolumen und diese Schätzungen vom globalen Marktvolumen gehen etwa von fünf Milliarden US-Dollar aus. Wenn man das methodisch genauer hinterfragt, kann man das vielleicht auch noch eher nach oben oder nach unten setzen. Dazu gibt es eine sehr empfehlenswerte, neue, vor kurzem erschienene Studie von dem Stockholmer Friedenforschungsinstitut Sipri, in der das auch noch einmal methodisch sowohl nach oben als auch nach unten hinterfragt wird. Also ob das mehr oder weniger als fünf Milliarden sind. Das ist sehr lesenswert, aber es gibt, denke ich, einen ungefähren Richtwert. Und wenn wir noch einmal über Deutschland sprechen, dann sehen wir hier ungefähr 20 Firmen, die sowohl Hard- als auch Software in dem Bereich exportieren. Und es gibt ungefähr 15 Firmen, die weltweit nur Trojanersoftware exportieren und da ist nach wie vor Deutschland, denke ich, relativ führend mit einigen Anbietern, rein von der technologischen Kompetenz und rein von dem Wissen, was auch mit Ausbildung, Bildung und Standorten zu tun hat. Auch München ist ein bekannter IT-Standort. Und wenn man es jetzt noch einmal in Arbeitsplätzen ausdrückt, vielleicht zielte die Frage dahin, wird eine signifikante Anzahl von Mitarbeitern, nach allem was wir von unseren Recherchen und was es auch an Marktberichten gibt, eigentlich nicht in Deutschland beschäftigt. Trovicor aus München gilt in Deutschland nach wie vor als eines der größten Unternehmen und beschäftigt, das hatte ich glaube vorhin auch schon gesagt, rund 170 Mitarbeiter. Damit sind die schon relativ groß. Aber 170 Mitarbeiter sind eigentlich nicht wirklich viel. Sofern wir neben der Frage nach der Regulierung die Frage nach Beschäftigungseffekten stellen oder wie sich das auf den Arbeitsmarkt auswirkt, würde ich auch immer sagen, signifikante negative Beschäftigungseffekte sind durch weitere Regulierungen eigentlich nicht

wirklich zu erwarten. EU-weit gehen wir von rund 200 Unternehmen in dem Bereich Hard- und Software aus.

Der **Vorsitzende:** Gibt es weitere Wortmeldungen? Kollege Schipanski, bitte schön.

Abg. Tankred Schipanski (CDU/CSU): Daran anknüpfend, aber an den Herrn Dr. Wagner die Frage gebend. Wir haben wahrscheinlich nicht nur Bayern, die da Cyber-Sicherheitsforschung betreiben. Wie verhält sich das im gesamteuropäischen oder weltweiten Kontext? Ich nehme an, die Asiaten und die Amerikaner werden auch mit gewissen Lösungen arbeiten und diese auch entsprechend präsentieren. Wir haben uns jetzt sehr auf die nationale Regulierung fokussiert, aber wie sprechen die Zahlen, sagen wir mal, weltweit prozentual? Sind wir diesbezüglich sehr weit vorne oder sehr stark? Und wie sieht das auf anderen Kontinenten aus?

Der **Vorsitzende:** Herr Dr. Wagner.

SV **Dr. Ben Wagner**: Es ist von den Daten her, die dazu vorliegen, relativ schwer einzuschätzen, wie Herr Mihr schon gesagt hat. Aber grob geschätzt aus den bisherigen Erkenntnissen ist es so, dass ein Großteil der betroffenen Software aus Nordamerika oder aus Europa kommt. Es gibt zunehmend Entwicklungen, wie Herr Dr. Gaycken schon angeführt hat, dass jetzt in Indien oder in China entsprechende Technologien entwickelt werden. Aber der Großteil des Marktes ist weiterhin von Europa und den USA dominiert. Wie schon gesagt wurde, ist die Mitarbeiterzahl von den betroffenen Technologien sehr klein und man muss das auch in Kontext setzen. Also wenn man sich vorstellt, dass ein paar hundert Leute einen Schaden bei Tausenden, die direkt, oder bei Millionen, die indirekt davon betroffen sind, anrichten, wird deutlich wie das Verhältnis einer relativ „kleinen“ Mitarbeiterzahl im Vergleich zur Gesamtwirtschaft Industrie ist. Gleichzeitig ist immer wieder auch von der Bundesregierung vor einigen Jahren argumentiert worden, dass das es einen Zukunftsmarkt für zivile Sicherheitstechnologie gäbe, den es ja zu fördern gelte. Und das ist natürlich die Schwierigkeit, dass ein sehr kleiner Markt dann, wenn er auch noch mit Hermesbürgschaften gefördert wird, wie wir das schon gehört haben oder mit ähnlichen Dingen, dann sehr schnell über sich hinauswächst und größer aussieht als er eigentlich erst einmal ist. Das ist weiterhin ein relativ kleiner Markt, der noch dazu weiterhin von relativ hohen Standards lebt, einfach deswegen, weil, wenn man schon diese Überwachung machen will, man meistens auch relativ schwache Anwender hat. Das heißt, die Polizei oder die Geheimdienste vor Ort haben schon oft Probleme bei dem Bedienen von Computern, ganz zu schweigen bei dem Bedienen komplexer Technologie. Das bedeutet, es müssen dann sehr fortgeschrittene Gesamtpakete geschnürt werden und diese Gesamtpakete, wie man sich die vorstellt, sind relativ schwer von anderen Unternehmen zu entwickeln. Grundsätzlich ist natürlich diese Abwanderungsbewegung möglich, also rein technisch gesehen. De facto ist sie bisher nicht so stark zu beobachten. Und es wäre etwas problematisch, würde man jetzt anfangen zu sagen, weil es abwandern könnte, würden wir nicht regulieren. Dann könnte man immer die Hände in den Schoß legen und sagen, technisch ist es möglich und wir sind zwar Marktführer, aber wir könnten es bald nicht mehr sein.

Der **Vorsitzende:** Herr Mihr und Herr Dr. Gaycken möchten gerne ergänzen.

SV **Christian Mihr**: Eine gute Ergänzung zu der Frage auch im internationalen Vergleich: Ein Akteur, den wir mit zunehmender Sorge betrachten, ist tatsächlich Russland in dem Bereich. Russland hat zum einen Wassenaar noch nicht implementiert und zum anderen hat es tatsächlich auch eine lebendige Industrie. Russland exportiert nicht nur diese Technologie. Das beobachten wir mit Sorge. Wir beobachten weltweit, dass Russland mehrere Gesetze exportiert, auch NGO-Gesetze. Das führt dazu, dass es Shrinking Spaces gibt, also dass Freiräume für die Zivilgesellschaft verengt werden. Und was wir in dem Zusammenhang auch beobachten, ist, dass Russland in Mexiko, Ecuador und anderen lateinamerikanischen Ländern auch zunehmend Politikberatung macht zu Lawful Interception. Es geht also darum, wie man Gesetze strikt, damit Überwachungstechnik illegitimer Weise eingesetzt wird. Das beobachten wir tatsächlich weltweit mit Sorge, dass der Import der NGO-Gesetze, was ja als ein russisches Erfolgsmodel gilt, auch mit dem Import oder Export von

Lawful Interception Gesetzen einhergeht. Das ist vielleicht noch so ein ganz genereller Trend, den man auch politisch noch einmal etwas in den Blick nehmen sollte und könnte.

Der **Vorsitzende:** Herr Dr. Gaycken.

SV **Dr. Sandro Gaycken**: Ich wollte auch noch einmal auf die Rolle Russlands und Asiens eingehen. Diese kommen sehr stark, das sehen wir ganz klar. Sie werden auch ganz stark gefördert. Man sieht das zum Beispiel auch in der Wissenschaft, wenn man sich ansieht, dass in der Publikationslandschaft zu Lawful Interception sehr, sehr viel aus Asien kommt. Es gibt also massive Finanzierungen in diesem Bereich und natürlich auch in Firmen. Und natürlich wollen die auch mit diesen Firmen skalieren und werden also auch in andere Regime exportieren. Und von daher wird ein Markt aufgebaut, der dann sowieso außerhalb der „Like-Minded“ Staaten, die sich um Exportkontrolle sorgen, liegt. Das ist also ein schwieriges Problem. Dazu kommt noch, dass wir einige neue große Spieler haben, die hatte Dr. Ben Wagner nicht erwähnt, die jetzt versuchen, da irgendwie mitzuspielen. Cisco zum Beispiel bietet neuerdings ein Lawful Interception-Programm an. Auch North Grumman will jetzt ganz groß dabei sein bei Cyber Security und bietet Lawful Interception an. Das sind dann allerdings auch wieder kleine Sparten in diesen großen Dingern. Also auch da sind die Abteilungen nicht größer als zwanzig, dreißig Leute. Von daher ist nicht der Konzern als Ganzes gefährdet. Aber man sieht doch, dass diese großen Konzerne versuchen, das mit ihren Konzernstrukturen aufzuarbeiten und auch anzubieten.

Der **Vorsitzende:** Ja, vielen Dank. Gibt es weitere Fragen oder Ergänzungen? Wenn das nicht der Fall ist, dann würde ich vorschlagen, dass wir eine kleine Abschlussrunde machen in umgedrehter Reihenfolge. Herr Mihr würde diesmal beginnen und Herr Prof. Waidner würde enden, so dass Sie einfach noch einmal in maximal drei Minuten zusammenfassen können. Herr Mihr, Sie können beginnen, bitte schön.

SV **Christian Mihr**: Ich glaube, das kriege ich auch in weniger als drei Minuten hin, weil wir die wesentlichen Punkte bereits gesagt haben und ich mich auch gar nicht auf ein Abschlussstatement vorbereitet habe. Aber trotzdem glaube ich, ich kann die wesentlichen Punkte noch einmal aus unserer Sicht von Reporter ohne Grenzen sagen. Die Technologie, über die wir hier reden, ist tatsächlich in den allermeisten Fällen eine menschenrechtsverachtende Technologie. Das muss man sich bei aller Diskussion über Dual-Use, glaube ich, immer vor Augen führen und tatsächlich auch die einzelnen Menschen im Blick behalten. Das ist der erste Punkt. Der zweite Punkt, der mir, glaube ich, wichtig ist und da möchte ich auch an das anknüpfen, was Herr Dr. Ben Wagner gesagt hat, ist diese Zurückhaltung und die mangelnde Transparenz, die wir hier haben. Dies wird oft angeführt, weil die Technologie so sensibel sei und weil der Politikbereich so sensibel sei. Dies ist mit Blick auf Finnland zum Beispiel überhaupt nicht angebracht und mehr Transparenz kann möglich sein. Drittens, ist es absolut zu begrüßen, dass Deutschland sich sehr engagiert hat in der Frage von Wassenaar und dort auch wirklich eine treibende Kraft war, diese Implementierung hier auch auf EU-Ebene umzusetzen. Überhaupt ist es begrüßenswert, dass es bei Wassenaar eine Einigung gegeben hat. Aber dazu gehören müsste eigentlich auch aus unserer Sicht, dass die Bundesregierung endlich auch ehrlich ist und alle Exportbürgschaften, die es im vergangenen Jahren gegeben hat, einmal auf den Tisch legt und sagt: „Hier haben wir auch Dreck am Stecken.“ Dass nicht immer nur auf Nachfragen von Journalisten, von NGOs und von Abgeordneten reagiert wird. Das wären aus meiner Sicht drei ganz wichtige Punkte.

Der **Vorsitzende:** Herr Dr. Wagner.

SV **Dr. Ben Wagner**: Zum Abschluss habe ich noch drei Punkte und dann, glaube ich, sind wir mit einer ganz guten Diskussion, die alle Punkte beleuchtet hat, im Wesentlichen am Ende. Ich glaube, ich würde gerne noch einmal darauf eingehen, was Herr Dr. Gaycken in seiner Stellungnahme und hier auch kurz noch einmal erwähnt hat, was auch auf die Frage von Herrn Wendt einging - dieser Kapazitätsaufbau von relevanten Institutionen. Das ist sehr sinnvoll und sehr notwendig. Im Rahmen des Arabischen Frühlings vor drei, vier Jahren gab es so eine Art Digital Hype. Mittlerweile stellt man jetzt fest, dass das politische Interesse an bestimmten Themen nicht mehr

ganz so groß ist und man sich deswegen jetzt gerade auch im Bereich der Außenpolitik andere Dinge anschaut. Das ist ein Problem und es führt auch dazu, dass den Institutionen die Kapazitäten auf solche komplexen Fragen zu reagieren, entzogen werden. Sie alle sind der Ausschuss Digitale Agenda. Ich muss es ja nicht überbetonen, aber diese Themen werden bleiben und sie werden nicht einfach so verschwinden und das hat insbesondere auch mit der internationalen Kooperation in diesem Bereich zu tun. Man kann digitale Themen gar nicht mehr sinnvoll in einem nationalen Kontext oder kaum europäisch betrachten, sondern eigentlich nur global und in einem sinnvoll globalen, vernetzten Kontext und da braucht es sowohl das Auswärtige Amt wie auch andere Institutionen innerhalb der Bundesregierung, die aktive Kapazitäten haben und diese auch nutzen. Der zweite Punkt soll nicht dem ersten widersprechen, aber das macht es doch ein bisschen komplexer. Wir hatten ja immer wieder das Thema Neutralität von glaubwürdigen Institutionen, das heißt, wie jetzt das Bundesamt für Sicherheit in der Informationstechnik oder auch andere Akteure, die eingebunden werden in diese Prozesse, sinnvoll und glaubwürdig agieren können. Und da muss man tatsächlich vorsichtig sein, weil es ja relativ normal ist für staatliche Institutionen ziemlich eng zu kooperieren. Aber gleichzeitig stellen sich auch gewisse Probleme in dem Moment, in dem es um den Verfassungsschutz oder auch andere Behörden geht, zum Beispiel Behörden wie dem Bundesamt für Sicherheit in der Informationstechnik. Aber auch Datenschutzbehörden in Deutschland, die dadurch weniger glaubwürdig werden. Und da muss man vorsichtig sein bei den bestehenden Kooperationen zwischen staatlichen Strukturen, um sicherzustellen, dass durch die Kooperation nicht entsprechend Glaubwürdigkeit entzogen wird. Und das ist der dritte oder abschließende Punkt. Wenn man glaubwürdig über Exportkontrolle und über Überwachungstechnologien sprechen will als Parlament, als Bundesregierung, als deutscher Staat, dann muss man das auch konsequent im Inland umsetzen und nicht nur im Ausland. Es reicht nicht über Exportkontrolle zu reden, sondern man muss genauso in Debatten über den sogenannten Bundestrojaner, der angeblich entwickelt werden soll und über verschiedene andere Techniken, die von den deutschen Polizeibehörden entwickelt werden, sehr gezielt hinschauen, um sicherzustellen, dass man die gleichen moralischen, ethischen und auch menschenrechtlichen Maßstäbe, die man ans Ausland stellt auch ans Inland stellt. Und dort müssen konsequent auch die entsprechenden Kontrollen genauso für deutsche Behörden gelten wie auch für ausländische.

Der **Vorsitzende:** Herr Prof. Dr. Neuneck, bitte schön.

SV **Prof. Dr. Götz Neuneck**: Vielen Dank. Ich glaube, es ist klar geworden, dass die Rüstungsexportkontrolle eine wichtige, aber auch eine begrenzte Funktion hat. Dass ein kontrollierter Umgang ganz wichtig ist, auch gerade, was die Endverbleibskontrolle angeht. Es zwingt die Staaten dazu Formulare auszufüllen und sich klar zu werden, unter welchen Kriterien sie liefern. Das wird nie ein Allheilmittel sein und muss erweitert werden. Es ist auch nur eine begrenzte Zahl von Staaten, die sich überhaupt dieser Rüstungsexportkontrolle unterwerfen und letztlich braucht man längerfristig Kriterien, auch global und international, um klar zu machen, unter welchen Bedingungen Überwachungssoftware legitim, legal ist und was die Kriterien sind. Es gibt dafür internationale Kriterien, die auch in der EU-Charta und den Menschenrechtskonventionen hinterlegt sind. Der Arms Trade Treaty sollte erweitert werden. Das bedarf auch international einiger Aktivitäten. Es muss kompatibel sein mit dem, was man innenpolitisch macht und ist ein zugfähiges Aufgabenfeld für Cyber Diplomacy.

Der **Vorsitzende:** Herr Dr. Gaycken.

SV **Dr. Sandro Gaycken:** Ich möchte einfach nur noch einmal betonen, dass ich Überwachung im Moment wirklich für die größte Gefahr für Demokratie und Menschenrechte halte. Weil wenn man sich in dieser Diskussion und in den Technologien befindet, man weiß, was die alle können, wie einfach die zu skalieren sind und wie einfach die zu modifizieren sind, dass man wirklich jeden Oppositionellen irgendwie fangen kann. Ich hatte in meiner Stellungnahme diesen Trend der Predictive Analytics erwähnt und es wurde mir auch einmal vorgeführt. Die geben also Namen ein und können relativ präzise sagen, wen er in den nächs-

ten sechs Monaten trifft, mit was er Netzwerke bildet oder auf was für dumme Ideen der kommen könnte. Das sind wahnsinnig gefährliche Technologien für die Demokratie sowie für die Menschenrechte. Von daher brauchen wir unbedingt mehr Aufmerksamkeit. Das kann eine autoritäre Herrschaft unglaublich stabilisieren. Das hat natürlich auch ganz harte sicherheitspolitische Implikationen, die dahinter stehen, nicht nur Menschenrechtsimplikationen für uns. Und wir müssen also dringend dieses Thema sehr viel intensiver beobachten und Vektoren finden, mit denen wir da herankommen. Spionagesoftwareexportkontrollen sind wichtig, aber bedürfen auch weiterhin des Ausbaus, der Beobachtung und der Kontrolle. Letzten Endes sind es aber das Internet, die Daten und das Smartphone selbst, die die Verräter sind und ich brauche gar nicht so gezielt diese Überwachungssoftware. Ich kann auch mit vielen anderen Sachen da herangehen und das ist einfach etwas, wo man ein bisschen mehr Aufmerksamkeit braucht und wo ich vor allem die Rolle der Cyber-Außenpolitik jetzt doch noch einmal stärken möchte. Dass ich das bedauerlich finde, dass ausgerechnet das jetzt eingespart wurde, vor allem, weil Deutschland auch eine führende Rolle hätte einnehmen können als Stimme für Freiheit, Menschenrechte und Demokratie im digitalen Raum. Und dass ausgerechnet da eingespart wurde, dass man ausgerechnet da jetzt sehr zögerlich und vorsichtig geworden ist, ist sehr bedauerlich.

Der **Vorsitzende:** Herr Prof. Waidner, bitte.

SV **Prof. Dr. Michael Waidner**: Vielen Dank. Gut, ich möchte ganz kurz drei Punkte noch einmal wiederholen. Also der erste Punkt ist, dass aus meiner Sicht Menschenrechte immer Vorrang haben müssen. Aber auch Schutz muss immer Vorrang haben. Es gibt aus meiner Sicht keine bessere Methode, Überwachungen in Unrechtstaaten zu bekämpfen als vernünftige Schutzmaßnahmen, Cyber-Sicherheit und dass Verschlüsselung freigegeben wird. Umgekehrt gilt auch, es wurde immer wieder angedeutet, dass solche Dinge wie Exploits unter die Exportkontrolle fallen sollten. Ich würde sagen, es gibt keinen vernünftigen ethischen Grund, warum Exploits überhaupt hergestellt werden. Von daher würde ich sie eigentlich radikal als Cyber-Crime verbieten. Der zweite Punkt ist, das habe ich schon erwähnt, Cyber-Sicherheit ist wichtig. Sie ist die beste Methode gegen Überwachung. Dementsprechend muss sie weiterhin gefördert und begünstigt werden. Und der dritte Punkt schließt an das an, was gerade schon gesagt worden ist. Wir haben darüber geredet, dass der Markt vielleicht fünf Milliarden sind. Das ist in Wirklichkeit natürlich eine Aussage, die man nicht treffen kann. Also der Markt für Überwachungstechnologie beinhaltet auch, Herr Dr. Gaycken hat es gerade angedeutet, Dinge wie, Big Data-Tools oder wie Smartphones. Von daher kann man sagen, die komplette IT kann zum Überwachen missbraucht werden. Von daher würde ich auch sagen, es ist weniger die Frage, ob es ein paar hundert Leute sind in Deutschland, die an dem Markt beteiligt sind. Auf die Branche, die nur Trojaner herstellt, könnte man gut verzichten. Da würde man tatsächlich nicht viel verlieren in Deutschland. Auf sowas wie die Herstellung von Big Data-Datenbanken von SAP und Software AG, auf die wollen wir wahrscheinlich nicht verzichten. Aber deswegen plädiere ich sehr dafür, bei der Definition von Überwachungssoftware und von Dingen, deren Export kontrolliert wird, sehr vorsichtig zu sein, sonst kommt man relativ schnell so weit, dass die komplette IT-Industrie exportkontrolliert wird. Vielen Dank.

Der **Vorsitzende:** Vielen herzlichen Dank. Mit diesen Ausführungen sind wir am Ende unserer heutigen Anhörung und der Sitzung des Ausschusses Digitale Agenda. Ich bedanke mich ganz herzlich bei den Sachverständigen für die wirklich außerordentlich interessanten Ausführungen, die sehr hilfreich sind für unsere Arbeit. Ich bedanke mich für das große Interesse hier bei den Zuhörern im Saal, aber auch natürlich auch denjenigen, die das im Livestream verfolgt haben. Ich bedanke mich ganz herzlich bei der Technik, die dafür gesorgt hat, dass der Livestream überhaupt möglich ist. Und da das die letzte Sitzung ist in diesem Jahr, wünsche ich allen eine wunderbare Adventszeit, frohe Weihnachten und natürlich ein gutes und glückliches Neues Jahr. Weihnachten kann es ruhig ein bisschen analog zugehen, mit einer echten Kerze und einem echten Weihnachtsbaum, mit handgemachter Musik usw. Also ich wünsche Ihnen alles Gute und bis zum nächsten Jahr. Die Sitzung ist geschlossen.

Schluss der Sitzung: 17:28 Uhr

Jens Koeppen, MdB
Vorsitzender